ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Κβαντικοί Υπολογιστές και Κβαντική Υπολογισιμότητα

Διπλωματική Εργασία του

Παναγιώτης Γρηγοριάδης

Επιβλέπων: Φώτιος Πλέσσας

1ος Συνεπιβλέπων: Διονύσιος Βαβουγυιός

2ος Συνεπιβλέπων: Γεώργιος Σταμούλης

Βόλος, 2020

ΠΑΝΕΠΙΣΤΗΜΙΟ ΘΕΣΣΑΛΙΑΣ

ΠΟΛΥΤΕΧΝΙΚΗ ΣΧΟΛΗ

ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

Κβαντικοί Υπολογιστές και Κβαντική Υπολογισιμότητα

Διπλωματική Εργασία του

Παναγιώτης Γρηγοριάδης

Επιβλέπων: Φώτιος Πλέσσας

1ος Συνεπιβλέπων: Διονύσιος Βαβουγυιός

2ος Συνεπιβλέπων: Γεώργιος Σταμούλης

Βόλος, 2020

UNIVERSITY OF THESSALY

POLYTECHNIC SCHOOL

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING

Quantum Computers and Quantum Computability

Thesis by

Panagiotis Grigoriadis

Advisor: Fotis Plessas

1st Coadvisor: Dionysis Vavougios

2nd Coadvisor: George Stamoulis

Volos, 2020

ΕΥΧΑΡΙΣΤΙΕΣ

Θα ήθελα να ευχαριστήσω την οικογένειά μου για την στήριξή της όλα αυτά τα χρόνια.

Παναγιώτης Γρηγοριάδης

ΥΠΕΥΘΥΝΗ ΔΗΛΩΣΗ ΠΕΡΙ ΑΚΑΔΗΜΑΪΚΗΣ ΔΕΟΝΤΟΛΟΓΙΑΣ ΚΑΙ ΠΝΕΥΜΑΤΙΚΩΝ ΔΙΚΑΙΩΜΑΤΩΝ

«Με πλήρη επίγνωση των συνεπειών του νόμου περί πνευματικών δικαιωμάτων, δηλώνω ρητά ότι η παρούσα διπλωματική εργασία, καθώς και τα ηλεκτρονικά αρχεία και πηγαίοι κώδικες που αναπτύχθηκαν ή τροποποιήθηκαν στα πλαίσια αυτής της εργασίας, αποτελεί αποκλειστικά προϊόν προσωπικής μου εργασίας, δεν προσβάλλει κάθε μορφής δικαιώματα διανοητικής ιδιοκτησίας, προσωπικότητας και προσωπικών δεδομένων τρίτων, δεν περιέχει έργα/εισφορές τρίτων για τα οποία απαιτείται άδεια των δημιουργών/δικαιούχων και δεν είναι προϊόν μερικής ή ολικής αντιγραφής, οι πηγές δε που χρησιμοποιήθηκαν περιορίζονται στις βιβλιογραφικές αναφορές και μόνον και πληρούν τους κανόνες της επιστημονικής παράθεσης. Τα σημεία όπου έχω χρησιμοποιήσει ιδέες, κείμενο, αρχεία ή/και πηγές άλλων συγγραφέων, αναφέρονται ευδιάκριτα στο κείμενο με την κατάλληλη παραπομπή και η σχετική αναφορά περιλαμβάνεται στο τμήμα των βιβλιογραφικών αναφορών με πλήρη περιγραφή. Αναλαμβάνω πλήρως, ατομικά και προσωπικά, όλες τις νομικές και διοικητικές συνέπειες που δύναται να προκύψουν στην περίπτωση κατά την οποία αποδειχθεί, διαχρονικά, ότι η εργασία αυτή ή τμήμα της δεν μου ανήκει διότι είναι προϊόν λογοκλοπής».

Γρηγοριάδης Παναγιώτης,

Φεβρουάριος, 2020

Περίληψη

Η κβαντομηχανική από μόνη της, αποτελεί ένα συναρπαστικό αντικείμενο ενδιαφέροντος, καθώς αποτελεί το θεμέλιο λίθο της ύπαρξης και του κόσμου, όπως τον ξέρουμε, και η πολυπλοκότητά της είναι τεράστια. Ο καμβάς πάνω στον οποίο ζωγραφίζει είναι ο διανυσματικός μιγαδικός χώρος Hilbert. Πάνω σε αυτόν περιγράφονται όλες οι κβαντικές καταστάσεις των φυσικών συστημάτων με τη χρήση κυρίως του συμβολισμού Dirac. Ωστόσο, ως μηχανικοί, σχεδόν ποτέ δεν ασχολούμαστε ή μαθαίνουμε κβαντομηχανικοί, καθώς στα συστήματα που αντιμετωπίζουμε οι κβαντομηχανικές ιδιότητες τους έχουν καταρεύσει και περιγράφονται ικανοποιητικά από την κλασσική φυσική. Μήπως μπορούμε να αξιοποιήσουμε αυτές τις ιδιότητες, εάν ασχοληθούμε με αρκετά ελαφριά και απομονωμένα συστήματα;

Η κβαντική υπολογιστική χρησιμοποιεί τις ιδιότητες της κβαντομηχανικής στην προσπάθεια επίλυσης προβλημάτων. Έχει αποδειχθεί θεωρητικά ότι προβλήματα όπως η αποστολή πληροφορίας, η τηλεμεταφορά, η μη δομημένη αναζήτηση σε βάσεις δεδομένων (αλγόριθμος του Grover) και η κρυπτογραφία (αλγόριθμος του Shor) μπορούν να αντιμετωπιστούν πολύ πιο αποδοτικά με τη χρήση κβαντικών αλγορίθμων. Και σε έναν κόσμο που βασίζεται στους υπολογιστές, η αύξηση της υπολογιστικής ισχύς αυτών είναι τεράστιας σημασίας. Αυτό ακριβώς υπόσχονται ότι θα κάνουν οι κβαντικοί υπολογιστές. Θα αποτελούν τη συσκευή πάνω στην οποία θα εκτελούνται κβαντικοί υπολογισμοί με την χρήση διαδοχικών κβαντικών πυλών για την επίλυση σημαντικών προβλημάτων.

Φυσικά αυτό δεν είναι εύκολο. Κατά τη διάρκεια ενός κβαντικού υπολογισμού προκύπτουν κβαντικά σφάλματα, καθώς κανένα μηχάνημα δεν είναι τέλειο. Η αναζήτηση τρόπων αντιμετώπισης των κβαντικών σφαλμάτων γενάει τον τομέα της κβαντικής διόρθωσης σφάλματος με απώτερο σκοπό την δημιουργία ενός κβαντικών κυκλωμάτων με ανοχή στο σφάλμα.

Η αναζήτηση της κατάλληλης τεχνολογίας για την κατασκευή κβαντικών υπολογιστών επίσης είναι περίπλοκη και διαφορετικές ερευνητικές ομάδες επιδιώκουν διαφορετικές ερευνητικές κατευθύνσεις. Το ποια, και εάν κάποια, επικρατήσει θα το δείξει ο χρόνος.

Λέξεις-κλειδιά: Κβαντομηχανική, κβαντικοί υπολογιστές, κβαντική υπολογισιμότητα, κβαντικό κύκλωμα, κβαντική πύλη, κβαντικός αλγόριθμος, κβαντικό σφάλμα, κβαντική διόρθωση σφάλματος, κβαντική ανοχή σφάλματος, κβαντική τηλεμεταφορά, κβαντική κρυπτογραφία, Grover, Shor

Abstract

Quantum Mechanics by itself is a fascinating subject of immense interest, as it is the building block of our own world and existance, as we know it. Its complexity, by all means, is huge. Quantum states of all physical systems exist on the complex Hilbert space and are described mainly with the help of the Dirac Notation. However, as engineers, we merely ever learn or have to deal with quantum mechanics, as the systems that we encounter have long abandoned their quantum properties and are described satisfyingly enough with classical mechanics. But maybe we can make good use of there properties, if we choose to investigate light and isolated enough systems.

Quantum computating uses the properties of quantum mechanics in its attempt to solve problems. It is proven theoretically that problems such as sharing information, teleportation, unstructured database search (Grover's algorithm) and cryptography (Shor's algorithm) can be coped with much more efficiently with the use of quantum algorithms. Of course, in a world that's based on computers, increasing their computational power is of huge importance. That's exactly what quantum computers promise. Quantum computers will be the apparatuses, on which quantum computations will be performed, with the use of quantum gates.

Such thing, of couse, is by no means easy. During a quantum computation quantum errors arise, as no machine is perfect. The search of how to deal with these errors gives birth to the sector of quantum error correction with ultimate purpose being the create of quantum circuits with quantum fault tolerance.

The search of the right technology to construct quantum computers is also highly complicated and different researching teams pursue different researching directions. Which, and if, one of them will prevail only time will tell.

Keywords: Quantum Mechanics, quantum computation, quantum computer, quantum circuit, quantum gate, quantum algorithm, quantum error, quantum error correction, quantum fault tolerance, quantum teleportation, quantum cryptography, Grover's algorithm, Shor's algorithm

Πίνακας περιεχομένων

ΚΕΦΑΛΑΙΟ 1

Εισαγωγή

Οι κβαντικοί υπολογιστές είναι υπολογιστικές μηχανές οι οποίες δυνητικά έχουν πολύ μεγαλύτερη υπολογιστική ισχύ από έναν κλασσικό υπολογιστή, ιδίως σε συγκεκριμένα προβλήματα. Αξιοποιούν τους νόμους της κβαντομηχανικής και οι αλγόριθμοι που τους αντιστοιχούν είναι πολύ λιγότεροι αλλά και πολύ διαφορετικοί από τους κλασσικούς αλγορίθμους ως προς τον τρόπο κατασκευής τους.

Ωστόσο, υπάρχει ήδη αρκετή θεωρία και αρκετοί αλγόριθμοι πάνω σε αυτούς που να καθιστά την ενασχόλιση με τον τομέα να αξίζει τον κόπο. Προβλήματα όπως η τηλεμεταφορά, η αναζήτηση σε αδόμητες βάσεις δεδομένων και η κρυπτογραφία φαίνεται να έχουν την δυνατότητα να επιταχυνθούν σημαντικά με την χρήση αυτών.

Η κατασκευή τους δεν είναι καθόλου απλό ζήτημα. Θεωρητικές, καθώς και τεχνικές δυσκολίες καραδωκούν σε κάθε γωνία. Από την αδυναμία αντιγραφής μιας κβαντικής κατάστασης στην προστασία ενός κβαντικού συστήματος από τον περιβαλλοντικό θόρυβο.

Αποτελούν αντικείμενο τεράστιου ενδιαφέροντος τα τελευταία χρόνια και τεράστια ποσά δαπανούνται στην έρευνα γύρω από αυτούς. Εταιρίες κολοσσοί όπως η Google και η IBM ηγούνται της προσπάθειας αυτής.

Ο σκεπτικισμός γύρω από αυτούς, καθώς και οι αμφιβολίες για το εάν ποτέ είναι εφικτό να φτιαχτεί ένας καθολικός κβαντικός υπολογιστής είναι μεγάλος.

Στο Κεφάλαιο 2, προσπαθώντας να δημιουργήσω μια στέρεα θεωρητική βάση, κάνω μια εισαγωγή στην κβαντομηχανική αναφέροντας κάποιες έννοιες, οι οποίες είναι απαραίτητες για την κατανόηση στην συνέχεια πιο περίπλοκων ζητημάτων σχετικά με τους κβαντικούς υπολογιστές.

Στο Κεφάλαιο 3 μπαίνω σε κάποια απλά και τελείως απαραίτητα εισαγωγικά στοιχεία της κβαντικής υπολογιστικής, τα οποία χρησιμεύουν ως εργαλεία σε οποιαδήποτε αναζήτηση στον χώρο αυτό.

Στο Κεφάλαιο 4 περιγράφω τα πιο γνωστά, εκ των πιο σύνθετων κβαντικών κυκλωμάτων και εφαρμογών, τα οποία έχουν εφευρεθεί, όπως η κβαντική τηλεμεταφορά.

Στο Κεφάλαιο 5 εστιάζω στα κβαντικά σφάλματα που συμβαίνουν κατά την πρακτική εφαρμογή ενός κβαντικού αλγορίθμου και στις τεχνικές που έχουν εφευρεθεί και χρησιμοποιούνται για την διόρθωση αυτών. Παρουσιάζω επίσης την έννοια της ανοχής σφαλμάτων.

Στο Κεφάλαιο 6 γυρνάω την προσοχή μου στις διάφορες κατευθύνσεις στην προσπάθεια κατασκευής ενός κβαντικού υπολογιστή.

Στο Κεφάλαιο 7 εγείρω τους προβληματισμούς μου σχετικά με τους κβαντικούς υπολογιστές και το κατά πόσο είναι εφικτή η κατασκευή ενός χρήσιμου κβαντικού υπολογιστή.

Στο Κεφάλαιο 8 κάνω μια σύντομη αναφορά στην πιο πρόσφατη και πολυαναμενόμενη εξέλιξη στον τομέα, την επίδειξη κβαντική υπεροχής.

Στο Κεφάλαιο 9 αναφέρω τα συμπεράσματά μου από την διεξοδική περιήγησή μου στον χώρο της κβαντικής υπολογιστικής το τελευταίο διάστημα.

ΚΕΦΑΛΑΙΟ 2

Γενικά στοιχεία κβαντομηχανικής

2.1 Τα αξιώματα της Κβαντομηχανικής

Αξίωμα 1 (σύνθετη συνάρτηση κατάστασης): *Κάθε φυσικό σύστημα περιγράφεται από μια συνάρτηση κατάστασης η οποία περιγράφει όλα όσα μπορούμε να γνωρίζουμε για το σύστημα. Αυτή είναι η κυματοσυνάρτηση $\psi(r, s, t)$, η οποία είναι μια ομάδα σύνθετων συναρτήσεων όλων των κλασσικών βαθμών ελευθερίας που δηλώνονται από τις ανεξάρτητες μεταβλητές r (διάνυσμα θέσης) και t (χρόνος) και των επιπλέον βαθμών ελευθερίας, όπως το s (spin), οι οποίοι είναι εγγενώς κβαντομηχανικοί. Δύο κυματοσυναρτήσεις αναπαριστούν την ίδια κατάσταση αν διαφέρουν μόνο κατά έναν παράγοντα φάσης ($e^{i\theta}$)* [1].

Αξίωμα 2 (η εξίσωση του Schrödinger): *Η χρονική εξέλιξη μιας κυματοσυνάρτησης ενός μη-σχετικιστικού φυσικού συστήματος δίνεται από την χρονικά εξαρτώμενη εξίσωση του Schrödinger:*

$i\hbar \frac{\partial \psi}{\partial t} = \hat{H}\psi$ *, όπου $\hat{H}$ είναι ο Χαμιλτονιανός Τελεστής, ο οποίος είναι γραμμικός ερμιτιανός τελεστής, του οποίου η έκφραση κατασκευάζεται από την αρχή της αντιστοιχίας* [1].

Αξίωμα 3 (αρχή της αντιστοιχίας): *Σε κάθε δυναμική μεταβλητή της Κλασσικής Μηχανικής αντιστοιχεί στην Κβαντική Μηχανική ένας γραμμικός ερμιτιανός τελεστής, ο οποίος όταν δρα πάνω στην κυματοσυνάρτηση, η οποία αντιστοιχεί σε μια ορισμένη τιμή του Παρατηρήσιμου (το ιδιοδιάνυσμα αντιστοιχεί σε μια ορισμένη ιδιοτιμή), φέρνει ως αποτέλεσμα αυτήν την τιμή επί την κυματοσυνάρτηση* [1].

Αξίωμα 4 (το αξίωμα του Von Neumann): *Αν μια μέτρηση πάνω σε ένα παρατηρήσιμο A δώσει κάποια τιμή a_j , τότε η κυματοσυνάρτηση του συστήματος αμέσως μετά την μέτρηση είναι το αντίστοιχο ιδιοδιάνυσμα (ιδιοκατάσταση) ψ_i* [1].

<u>Αξίωμα 5 (το αξίωμα του Born: πιθανοτική ερμηνεία της κυματοσυνάρτησης):</u> *Η τετραγωνική νόρμα της κυματοσυνάρτησης* $|\psi|^2$ *ερμηνεύεται ως η πιθανότητα το σύστημα να έχει τις τιμές (r, s), την χρονική στιγμή t* [1].

Αυτή η ερμηνεία προϋποθέτει ότι το άθροισμα των συνιστωσών $|\psi|^2$ για όλες τις *τιμές (r, s), την χρονική στιγμή t να είναι πεπερασμένο (δηλαδή οι φυσικά αποδεκτές κυματοσυναρτήσεις είναι τετραγωνικά ολοκληρώσιμες). Πιο συγκεκριμένα, αν* $\psi(r, s, t)$ *είναι η κυματοσυνάρτηση ενός σωματιδίου,* $\psi^*(\mathrm{r,s,t})\psi(\mathrm{r,s,t})\mathrm{dv}$ *είναι η πιθανότητα το σωματίδιο να βρίσκεται στο στοιχείο όγκου dv που βρίσκεται στην θέση r την χρονική στιγμή t. Εξαιτίας αυτής της ερμηνείας και αφού η πιθανότητα του να βρεθεί ένα σωματίδιο οπουδήποτε είναι 1, η κυματοσυνάρτηση πρέπει να ικανοποιεί την προϋπόθεση κανονικότητας:*

$$\int_{-\infty}^{+\infty} \psi^*(\mathrm{r,s,t})\psi(\mathrm{r,s,t})\mathrm{dv} = 1 \text{ [1]}$$

Σε αυτό το σημείο να σημειώσουμε ότι τα αξιώματα της κβαντομηχανικής ανάλογα την πηγή και το πού θέλει να εστιάσει ο συντάκτης, μπορεί να διαφέρουν τόσο σε αριθμό όσο και σε διατύπωση, αλλά εν τέλει περιγράφουν την ίδιο εικόνα. Δεν υπάρχει κάποιο μοναδικό σύνολο αξιωμάτων που να αναγνωρίζεται και να είναι αποδεκτό παγκοσμίως [2].

2.2 Συμβολισμός Dirac, χώρος καταστάσεων και βάση διανυσματικού χώρου

Οι καταστάσεις ενός κλειστού κβαντικού συστήματος περιγράφονται από ένα διάνυσμα $|\psi\rangle$ στον χώρο καταστάσεων, ο οποίος είναι γενικά ένας μιγαδικός χώρος Hilbert με διάσταση d, εξοπλισμένος με την πράξη του εσωτερικού γινομένου μεταξύ δύο διανυσμάτων $|\psi\rangle, |\chi\rangle$, η οποία ορίζεται μέσω της ακόλουθης συνάρτησης:

$$H \times H \to C: \langle\chi|\psi\rangle = \langle\psi|\chi\rangle \text{ [3]}$$

Πιο αναλυτικά, ο συμβολισμός που χρησιμοποιείται από την επιστημονική κοινότητα και θα χρησιμοποιώ για την περιγραφή της Κβαντικής Κατάστασης ενός κλειστού κβαντικού συστήματος από εδώ και έπειτα είναι ο συμβολισμός Dirac, γνωστός και ως Bra-Ket συμβολισμός.

Bra: $|\psi\rangle$

Ket: $\langle\psi|$ [4]

Τόσο το Bra όσο και το Ket συμβολίζουν ένα διάνυσμα σε ένα μιγαδικό διανυσματικό χώρο (Complex Vector Space) n διαστάσεων ($\mathbb{C}^n$), ο οποίος λέγεται Χώρος Χίλμπερτ (Hilbert Space) και μπορούν να περιγραφούν ως διάνυσμα στήλης ή γραμμής αντίστοιχα [4].

Χώρος Hilbert είναι ένα πραγματικός ή μιγαδικός διανυσματικός χώρος με δυνητικά άπειρη διάσταση ο οποίος:

1. Έχει την ιδιότητα του εσωτερικού γινομένου
2. Είναι πλήρης ως προς τη νόρμα που ορίζει το εσωτερικό γινόμενο

Πλήρης σημαίνει οποιαδήποτε ακολουθία Cauchy διανυσμάτων στον χώρο συγκλίνει σε κάποιο διάνυσμα επίσης σε αυτόν τον χώρο. Η δεύτερη ιδιότητα δεν θα μας απασχολήσει ιδιαίτερα οπότε δεν θα την εξηγήσουμε παραπάνω [5].

Η υπέρθεση δύο ή περισσότερων καταστάσεων αποτελεί, επίσης, μια πιθανή κατάσταση του κλειστού κβαντικού συστήματος:

$$|\psi\rangle = a_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + \alpha_3|\psi_3\rangle + \cdots, \text{ όπου } \alpha_1, \alpha_2, \alpha_3, \ldots \exists\ \mathbb{C} \quad [6]$$

-Αυτό από μόνο του καθιστά πρακτικά αδύνατη την οπτικοποίηση αυτόν των διανυσμάτων στις περισσότερες περιπτώσεις. Πώς μοιάζει ένας σύνθετος διανυσματικός χώρος, πόσο μάλλον n διαστάσεων; Ο συνήθης πραγματικός διανυσματικός χώρος (Real Vector Space) 2 διαστάσεων (x,y) που χρησιμοποιούμε, είναι ικανός να περιγράψει μόνο τον μιγαδικό διανυσματικό χώρο 1 διάστασης (z = x + iy). Αυτός είναι και ένας από τους βασικούς λόγους που όταν ασχολείσαι με την Κβαντομηχανική, είναι σημαντικό να επικεντρώνεσαι στα μαθηματικά και να τα «αφήνεις να μιλήσουν μόνα τους», εξού και η πολύ γνωστή έκφραση «shut up and do the math».-

Η διανυσματική βάση ενός χώρου Hilbert έχει ακριβώς την ίδια έννοια με οποιαδήποτε άλλη διανυσματική βάση ενός απλού διανυσματικού χώρου. Βάση ενός οποιουδήποτε διανυσματικού χώρου διάστασης N είναι ένα σύνολο διανυσμάτων $e_1, e_2, \ldots, e_N$, εάν κάθε διάνυσμα x αυτού του χώρου μπορεί να γραφεί ως:

$$x = x_1 e_1 + x_2 e_2 + \cdots + x_N e_N \ \ [7]$$

Έτσι, δωσμένης μιας βάσης του χώρου Hilbert που αντιστοιχεί στις καταστάσεις ενός φυσικού συστήματος, οποιοδήποτε διάνυσμα Ket μπορεί να εκφραστεί ως γραμμικός συνδυασμός των στοιχείων της βάσης.

$$|\psi\rangle = \sum_i c_i |k_i\rangle \ \ [7]$$

Όπου:

- c_i είναι μιγαδικοί αριθμοί και οι συντελεστές που αναπαριστούν το πλάτος πιθανότητας, έτσι ώστε: $\sum_i \left|c_i^2\right| = 1$
- $|\psi\rangle$ το διάνυσμα ket που θέλουμε να εκφράσουμε ως προς το διάνυσμα βάσης
- $|k_i\rangle$ τα διανύσματα ket της βάσης

Μια ειδική κατηγορία βάσεων είναι οι ορθοκανονικές βάσεις:

$$|e_1\rangle, |e_2\rangle, |e_3\rangle, \dots, |e_N\rangle \text{ , } \textit{όπου N είναι η διάσταση του χώρου}$$

Τα στοιχεία μιας ορθοκανονικής βάσης έχουν την ιδιότητα:

$$\langle e_i | e_j \rangle = \delta_{ij}$$

‘Οπου δ_{ij} είναι το Kronecker δέλτα για το οποίο ισχύει:

$$\delta_{ij} = \begin{cases} 0, \varepsilon\acute{\alpha}\nu\ i \neq j \\ 1, \varepsilon\acute{\alpha}\nu\ i = j \end{cases} \ \ [7]$$

Τα Bra, Ket είναι ερμιτιανά συζυγή, μεταξύ τους, διανύσματα. Μπορούν, εφόσον η διανυσματική βάση είναι διάκριτη να αναπαρασταθούν και ως πίνακες. Συγκεκριμένα, η σχέση που τα περιγράφει είναι η εξής:

Bra: $|\psi\rangle \rightarrow |\psi\rangle = \begin{bmatrix} \alpha \\ \beta \\ \gamma \\ \vdots \end{bmatrix}$, όπου $\alpha, \beta, \gamma, \dots \in \mathbb{C}$

Ket: $\langle\psi| \rightarrow |\psi\rangle^t = [\alpha^* \ \beta^* \ \gamma^* \dots]$, όπου $\alpha, \beta, \gamma, \dots \in \mathbb{C}$

Και η σχέση μεταξύ τους: $|\psi\rangle = \langle\psi|^H = \langle\psi|^t = (\langle\psi|^*)^T$ [4]

Τα α,β,γ,... (τα στοιχεία της στήλης) αποτελούν τις προβολές του $|\psi\rangle$ κατα μήκως των διευθύνσεων του διανύσματος βάσης [4].

2.3 Εσωτερικό γινόμενο διανυσμάτων (Inner Product)

Στο χώρο Hilbert ορίζεται το εσωτερικό γινόμενο διανυσμάτων. Το εσωτερικό γινόμενο των διανυσμάτων Bra, Ket, δηλαδή το Bra-Ket αποδεικνύεται πολύ χρήσιμο, καθώς συνδέεται με τις έννοιες του πλάτους και της πιθανότητας κατάρρευσης ενός Κβαντικού Συστήματος σε μια Κατάσταση μετά από μια Μέτρηση, πράγματα που θα δούμε στην πορεία. Για την ώρα, ας μείνουμε στο ότι το εσωτερικό γινόμενο είναι το εξής:

$$\langle\psi|\varphi\rangle = \begin{bmatrix}\alpha_1\\ \alpha_2\\ \vdots\end{bmatrix} * \ [\beta_1^* \ \beta_2^* \dots] = \beta_1^*\alpha_1 + \beta_2^*\alpha_2 + \cdots$$

Και ισχύει :

$$\langle\psi|\varphi\rangle = \int dx\psi^*(x)\varphi(x) \ \text{[4]}$$

2.4 Μέθοδοι τελεστών στην κβαντομηχανική (Quantum Operators)

Οι τελεστές κάνουν «κάτι» πάνω σε ένα διάνυσμα.

Σε κάθε φυσικό μέγεθος (θέση, ορμή, ενέργεια, κτλπ...) αντιστοιχεί ένας γραμμικός μετασχηματισμός στο χώρο Hilbert, ο οποίος δρα πάνω σε ένα Ket διάνυσμα, το οποίο περιγράφει το σύστημα.

$$\widehat{A} : |\psi\rangle \rightarrow \ |\psi'\rangle = \widehat{A}\,|\psi\rangle \ \text{[3]}$$

Συμβολίζεται συνήθως με κεφαλαίο γράμμα και «καπέλο» (π.χ. $\hat{A}$), αν και συχνά το καπέλο αγνοείται (όπως θα το αγνοώ και εγώ από το 2.11 και έπειτα). Ο γραμμικός τελεστής που αντιστοιχεί σε φυσικά μεγέθη πρέπει να είναι ερμιτιανός τελεστής, δηλ. να ισχύει:

$$\hat{A}^t = \hat{A}, \text{όπου } \hat{A}^t = \overline{A^T} \ \text{[3]}$$

Ο λόγος γι’ αυτό είναι ότι όλοι οι ερμιτιανοί τελεστές έχουν ιδιοδιανύσματα και μόνο οι ερμιτιανοί τελεστές έχουν πραγματικές ιδιοτιμές, κάτι που είναι απαραίτητη προϋπόθεση για

ένα μετρήσιμο φυσικό μέγεθος. Αυτό, περιγράφεται από την κλασσική εξίσωση ιδιοτιμών και ιδιοδιανυσμάτων:

$$\hat{A}\,|\lambda\rangle = \lambda\,|\lambda\rangle$$

όπου:

- $\hat{A}$ *= Ερμιτιανός Τελεστής*
- λ *= Ιδιοτιμή του Ερμιτιανού Τελεστή* ($\lambda_1, \lambda_2, \dots, \lambda_n$)
- $|\lambda\rangle$ *= Ιδιοδιάνυσμα του Ερμιτιανού Τελεστή* ($|\lambda_1\rangle, |\lambda_2\rangle, \dots, |\lambda_n\rangle$) [3]

Στην κβαντομηχανική, όταν κάνουμε κάποια μέτρηση ενός φυσικού μεγέθους σε ένα κλειστό κβαντικό σύστημα, στην ουσία εκτελούμε μια μέτρηση στο παρατηρίσιμο , το οποίο αντιστοιχεί σε έναν ερμιτιανό τελεστή. Οι πιθανές τιμές του παρατηρήσιμου $\widehat{\mathrm{A}}$ είναι οι Ιδιοτιμές λ του αντίστοιχου ερμιτιανού τελεστή [3].

Οι καταστάσεις στις οποίες το παρατηρήσιμο έχει μια συγκεκριμένη, βέβαιη, προβλέψιμη τιμή -δηλαδή μια τιμή που κατά την μέτρηση αντιστοιχεί σωστά στην κατάσταση που προετοίμασα το σύστημα- είναι τα Ιδιοδιανύσματα του ερμιτιανού τελεστή $|\lambda\rangle$ [3].

Η πιθανότητα να ληφθεί μία από τις ιδιοτιμές λ_i ενός τελεστή ως αποτέλεσμα μίας μοναδικής μέτρησης ενός παρατηρήσιμου πάνω σε ένα κλειστό κβαντικό σύστημα που βρίσκεται σε μία γενική κατάσταση $|\psi\rangle$ δίνεται από το τετράγωνο του μέτρου της προβολής της $|\psi\rangle$ πάνω στο αντίστοιχο ιδιοδιάνυσμα $|\lambda_i\rangle$ του τελεστή:

$$Prob(\lambda_i) = |\langle\lambda_i|\psi\rangle|^2 = \langle\psi|\lambda_i\rangle\,\langle\lambda_i|\psi\rangle \geq 0$$ [3]

2.5 Εξωτερικό γινόμενο διανυσμάτων / Δυάδα (Outer Product / Dyad)

Το εξωτερικό γινόμενο ή η δυάδα διανυσμάτων είναι ένας γραμμικός, μη ερμιτιανός τελεστής που εφαρμόζεται πάνω σε ένα διάνυσμα και ορίζεται ως:

$$|\chi\rangle\langle\psi|$$ [7]

Για παράδειγμα εάν το εφαρμόσουμε στο διάνυσμα $|\varphi\rangle$ παίρνουμε:

$$[|\chi\rangle\langle\psi|]\,|\varphi\rangle = |\chi\rangle\,\langle\psi|\varphi\rangle$$

Όπου:

- $|\chi\rangle$ είναι διάνυσμα
- $\langle\psi|\varphi\rangle$ είναι ένας αριθμός

Επίσης, αν έχω μια βάση από διανύσματα $|n\rangle$, μπορώ να γράψω οποιοδήποτε διάνυσμα $|v\rangle$ σε αυτήν:

$$|v\rangle = \sum v_n|n\rangle = \sum|n\rangle\langle n||v\rangle = \pi\rho o\beta o\lambda\acute{\eta}\ \tau o\upsilon\ |v\rangle\ \pi\acute{\alpha}\nu\omega\ \sigma\tau o\ |n\rangle$$

Όπου:

- v_n είναι οι συντελεστές των διανυσμάτων της βάσης [7]

Άρα μπορώ να ερμηνεύσω το $\sum_n|n\rangle\langle n|$ ως τον ταυτοτικό τελεστή I:

$$\sum_n |n\rangle\langle n| = 1 = I$$

Δηλαδή, ο ταυτοτικός τελεστής είναι το αθροισμα πάνω σε μια βάση δυάδων [7].

2.6 Κυματοσυνάρτηση (Wavefunction)

Ένας εναλλακτικός τρόπος να περιγράψεις την κατάσταση ενός κβαντικού συστήματος είναι η κυματοσυνάρτηση [4].

Τι είναι, όμως, μια κβαντική κυματοσυνάρτηση;
Υπενθυμίζουμε: Όλα τα κβαντικά σωματίδια συμπεριφέρονται, πάντα, ως κύματα.
Άρα μήπως η κυματοσυνάρτηση αυτή περιγράφει κάποια ιδιότητα του σωματιδίου; Όχι ακριβώς [4].

Η κβαντική κυματοΣυνάρτηση είναι μια μαθηματική οντότητα η οποία δεν έχει κάποια φυσικό νόημα. Ωστόσο αν την πολλαπλασιάσεις με το συζυγές της (ύψωση στο τετράγωνο), παίρνει το νόημα της κατανομής πιθανότητας, για την ιδιότητα που έχει ως είσοδο. Η συνολική επιφάνεια

που καλύπτεται σε μια γραφική παράσταση από την κατανομή πιθανότητας συναρτήσει της ιδιότητας που μας ενδιαφέρει είναι πάντα 1 (100%) [4].

Η κυματοσυνάρτηση παίρνει μιγαδικές τιμές και εκφράζει το πλάτος πιθανότητας. Μέσω αυτής παίρνουμε τις πιθανότητες για τα πιθανά αποτελέσματα διαφόρων μετρήσεων που μπορούν να γίνουν στο σύστημα [4].

Αυτό, στη βάση θέσης (Position Base), εκφράζεται με τις σχέσεις:

$\psi(x) = \langle x|\psi\rangle$ [4]

$P(x_0) = |\psi(x_0)|^2 = \psi(x_0)^*\psi(x_0) = \langle x_0|\psi\rangle^2 = \langle x_0|\psi\rangle\langle\psi|x_0\rangle$ [4]

Αφού η συνολική πιθανότητα να βρούμε το κβαντικό μας σύστημα (πιθανότατα κάποιο σωματίδιο) κάπου πρέπει να είναι 1, δηλαδή το άθροισμα τον πιθανοτήτων σε όλα τα σημεία του χώρου, η κυματοσυνάρτηση πρέπει πάντα να είναι κανονικοποιημένη:

$$\int dr\psi^*(r)\psi(r) = 1 \quad \text{(Συνθήκη Κανονικοποίησης)} \ [4]$$

Αντίστοιχα, η κυματοσυνάρτηση μπορεί να εκφραστεί συναρτήσει άλλων ιδιοτήτων του συστήματος που μας ενδιαφέρει, όπως η ορμή, η ενέργεια, η γωνιακή ορμή κτλπ. και να μας δώσει την πιθανότητα το σύστημα να έχει μια συγκεκριμένη τιμή της εκάστοτε ιδιότητας.

2.7 Αναμενόμενη Τιμή

Με τον όρο αναμενόμενη τιμή, ο οποίος μάλλον θα ήταν πιο ακριβής ως «μέση τιμή», υπολογίζω την μέση τιμή των πιθανών ιδιοτιμών ενός παρατηρήσιμου $\widehat{A}$ σε μια κατάσταση $|\psi\rangle$ [7]. Ισχύει:

$$\langle\psi|\hat{A}|\psi\rangle = \sum_1^n P_n\lambda_n = \bar{\lambda} = \bar{A} = \langle A\rangle$$

Όπου:

- λ_n *η ν-οστή ιδιοτιμή του* $\bar{A}$
- P_n *η πιθανότητα αν μετρήσω το* $\bar{A}$ *να πάρω την* λ_n

- $\bar{\lambda}$ *η μέση τιμή των ιδιοτιμών του* $\hat{A}$
- $\bar{A}$ *η μέση τιμή του* $\hat{A}$
- $\langle A \rangle$ *η Expectation Value του* $\hat{A}$ [7]

2.8 Μεταθέτης και Αντιμεταθέτης (αντι-Μεταθέτης)

Ο μεταθέτης μεταξύ δύο τελεστών $\hat{A}, \hat{B}$ ορίζεται ως:

$$\left[\hat{A}, \hat{B}\right] = \hat{A}\hat{B} - \hat{B}\hat{A}$$

Ο Α μετατίθεται με το Β όταν:

$$\left[\hat{A}, \hat{B}\right] = 0 => \hat{A}\hat{B} = \hat{B}\hat{A}$$

Ο αντιμεταθέτης μεταξύ δύο τελεστών Α, Β ορίζεται ως:

$$\left\{\hat{A}, \hat{B}\right\} = \hat{A}\hat{B} + \hat{B}\hat{A}$$

Το Α αντι-μετατίθεται με το Β όταν:

$$\left\{\hat{A}, \hat{B}\right\} = 0 => \hat{A}\hat{B} = -\hat{B}\hat{A}$$ [8]

Όταν δύο τελεστές $\hat{A}, \hat{B}$ μετατίθονται, τότε μπορούν και οι δύο να εκφραστούν ως προς μια κοινή ορθοκανονική βάση ιδιοδιανυσμάτων $|i\rangle$ ως εξής:

$$\hat{A} = \sum_i a_i |i\rangle\langle i|$$
$$\hat{B} = \sum_i b_i |i\rangle\langle i|$$ [8]

2.9 Χρονική Εξέλιξη και Εξίσωση Schrodinger

Η χρονική εξέλιξη μιας κατάστασης ενός συστήματος βρίσκεται λύνοντας την εξαρτώμενη από τον χρόνο εξίσωση του Schrodinger :

$i\hbar \frac{\partial \psi}{\partial t} = \widehat{H}\psi$ *, όπου* $\widehat{H}$ *είναι ο χαμιλτονιανός τελεστής* [7]

Να σημειώσω σε αυτό το σημείο ότι η παραπάνω είναι η γενική μορφή της εξίσωσης, και μιας και δεν θα μπούμε σε πολύ βαθειά μαθηματικά και περίπλοκα παραδείγματα φυσικής, δεν θα την αναλύσουμε παραπάνω.

2.10 Κβαντικό Spin

Το spin (ή intrinsic angular momentum, δηλαδή ιδιοστροφορμή) είναι μια εγγενής ιδιότητα όλων των στοιχειωδών σωματιδίων. Δεν σημαίνει ότι τα σωματίδια πραγματικά περιστρέφονται, αλλά είναι μια ακριβής αναλογία. Τα σωματίδια έχουν στροφορμή και κάποιο προσανατολισμό στο χώρο [7].

Το spin ενός σωματιδίου μπορεί να μετρηθεί, αλλά πρέπει να διαλέξουμε την διεύθυνση ως προς την οποία θα το μετρήσουμε. Έτσι, η μέτρηση μπορεί να έχει μόνο δύο αποτελέσματα. Είτε το spin θα είναι πάνω (up, δηλαδή $spin = \frac{\hbar}{2}$), δηλαδή ευθυγραμμισμένο με τη διεύθυνση μέτρησης, είτε κάτω (down, δηλαδή $spin = -\frac{\hbar}{2}$), δηλαδή αντίθετο με τη διεύθυνση μέτρησης [4].

Τι γίνεται αν μετρήσουμε όμως το spin ως προς διεύθυνση διαφορετική από τη διεύθυνση του spin του σωματιδίου; Τότε σύμφωνα με κάποιες πιθανότητες που προκύπτουν από την Κβαντομηχανική, το σωματίδιο μπορεί να έχει πλέον spin up ή spin down. Μετά την μέτρηση το σωματίδιο διατηρεί αυτό το spin [8].

Όταν θέλουμε, λοιπόν, να περιγράψουμε μια κβαντική κατάσταση βάση του spin σε κάποιον άξονα (z,x,y) χρησιμοποιούμε τους τελεστές spin S_z, S_x, S_y , οι οποίοι περιγράφονται από τις μήτρες του Pauli (τις οποίες θα δούμε στο κεφάλαιο 3.8) και έχουν ιδιοτιμές $\frac{\hbar}{2}$ και διανύσματα βάσης αντίστοιχα $|\mp z\rangle, |\mp x\rangle, |\mp y\rangle$ [8].

$$S_z = \frac{\hbar}{2}\sigma_z = \frac{\hbar}{2}\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix}, \mu\varepsilon\ \iota\delta\iota o\delta\iota\alpha\nu\acute{\upsilon}\sigma\mu\alpha\tau\alpha\ |+z\rangle = \begin{bmatrix}1\\0\end{bmatrix}, |-z\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

$$S_x = \frac{\hbar}{2}\sigma_x = \frac{\hbar}{2}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}, \mu\varepsilon\ \iota\delta\iota o\delta\iota\alpha\nu\acute{\upsilon}\sigma\mu\alpha\tau\alpha\ |+x\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix}, |-x\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-1\end{bmatrix}$$

$$S_y = \frac{\hbar}{2}\sigma_y = \frac{\hbar}{2}\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}, \mu\varepsilon\ \iota\delta\iota o\delta\iota\alpha\nu\acute{\upsilon}\sigma\mu\alpha\tau\alpha\ |+y\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\i\end{bmatrix}, |-y\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\-i\end{bmatrix}\ [8]$$

Παράδειγμα:

Έστω ένα σωματίδιο, το οποίο έχουμε προετοιμάσει σε κάποια κανονικοποιημένη κατάσταση

$|\psi\rangle = \begin{bmatrix} \frac{4}{5}i \\ \frac{9}{25} - \frac{12}{25}i \end{bmatrix}$. Ποια είναι η πιθανότητα να μετρήσουμε την κατάσταση του σωματιδίου ως spin = up , στον z-άξονα;

Διεξάγουμε μια μέτρηση κατά τον z άξονα. Το πλάτος πιθανότητας προκύπτει ως εξής:

$$\langle +z|\psi\rangle = \begin{bmatrix} 1 & 0 \end{bmatrix} \begin{bmatrix} \frac{4}{5}i \\ \frac{9}{25} - \frac{12}{25}i \end{bmatrix} = \frac{4}{5}i$$

Η πιθανότητα, τώρα, το σωματίδιο να έχει $spin = +\frac{\hbar}{2}$ είναι:

$$P(up, z\_axis) = |\langle +z|\psi\rangle|^2 = \left(\frac{4}{5}i\right)^2 = \left(\frac{4}{5}i\right) \times \left(\frac{4}{5}(-i)\right) = \frac{16}{25} = 64\%$$

Αντίστοιχα η πιθανότητα το σωματίδιο να έχει $spin = -\frac{\hbar}{2}$ είναι:

$$P(down, z\_axis) = |\langle -z|\psi\rangle|^2 = \frac{9}{25} = 36\%$$

Η αναμενόμενη τιμή κατά την μέτρηση στον z-άξονα είναι:

$$\langle S_z\rangle = \langle\psi|\widehat{S_z}|\psi\rangle = \sum_1^n P_n\lambda_n = 0.64 \times \frac{\hbar}{2} + 0.36 \times \frac{-\hbar}{2} = 0.28\frac{\hbar}{2} = 0.14\hbar$$

Με τον ίδιο τρόπο ακριβώς, χρησιμοποιώντας τα διανύσματα βάσης των άλλων αξόνων, μπορούμε να υπολογίσουμε την πιθανότητα το σωματίδιο να έχει spin up/down και την αναμενόμενη τιμή του, μετά την πράξη της μέτρησης, κατά τους άξονες x,y.

2.11 Κβαντική Διεμπλοκή (Quantum Entanglement)

Η κβαντική διεμπλοκή είναι ένα φυσικό φαινόμενο κατά το οποίο η κβαντική κατάσταση κάποιων κβαντικών συστημάτων (σωματιδίων) δεν μπορεί να γραφεί ως τανυστικό γινόμενο των βασικών τους καταστάσεων (δηλαδή δεν μπορεί να περιγραφεί ξεχωριστά για το καθένα, αλλά μόνο για όλα μαζί) [9].

Οποιαδήποτε κβαντική κατάσταση δεν μπορεί να διασπαστεί σε κομμάτια, λέγεται entangled state. Ας δούμε ένα παράδειγμα για το τι σημαίνει αυτό:

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \neq (\alpha|0\rangle + \beta|1\rangle) \otimes (\gamma|0\rangle + \delta|1\rangle)\,,$$

όπου $(\alpha|0\rangle + \beta|1\rangle)$ *είναι το πρώτο qubit και* $(\gamma|0\rangle + \delta|1\rangle)$ *είναι το δεύτερο qubit, καθώς:*

$$\begin{bmatrix}\alpha\\ \beta\end{bmatrix} \otimes \begin{bmatrix}\gamma\\ \delta\end{bmatrix} = (\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) = \alpha\gamma|00\rangle + \alpha\delta|01\rangle + \beta\gamma|10\rangle + \beta\delta|11\rangle\,,$$

δηλαδή:

$$\alpha\gamma = \frac{1}{\sqrt{2}} \; \kappa\alpha\iota \; \beta\delta = \frac{1}{\sqrt{2}} \; \kappa\alpha\iota \; \alpha\delta = \beta\gamma = 0,$$

το οποίο είναι άτοπο.

Οι entangled states είναι πάρα πολύ σημαντικές για τους κβαντικούς υπολογισμούς [8] και επιτυγχάνονται με την χρήση πυλών Hadamard και CNOT, κάτι που δείχνουμε στο κεφάλαιο 3.6.4.

2.12 Τελεστής/Μήτρα Πυκνότητας (Density Operator/Matrix)

Ο τελεστής πυκνότητας είναι ένας εναλλακτικός, ισοδύναμος τρόπος για να περιγράφουμε ένα κβαντικό σύστημα του οποίου την κατάσταση δεν γνωρίζουμε ακριβώς [10].

Έστω ότι έχουμε ένα σύστημα σε μία εκ των καταστάσεων $|\psi_i\rangle$, όπου i είναι δείκτης, με αντίστοιχες πιθανότητες p_i.
Αποκαλούμε την ποσότητα $\{p_i|\psi_i\rangle\}$ σύνολο καθαρών καταστάσεων (ensemble of pure states[1]).
Ο τελεστής πυκνότητας του συστήματος ορίζεται ως:

$$\rho \equiv \sum_i p_i|\psi_i\rangle\langle\psi_i| \quad [10]$$

Τα αξιώματα της Κβαντομηχανικής μπορούν να αναδιατυπωθούν σε σχέση με τον τελεστή πυκνότητας [10].

Η εξέλιξη ενός κβαντικού συστήματος, η οποία περιγράφεται από τον μοναδιαίο τελεστή U, με χρήση του τελεστή πυκνότητας, περιγράφεται ως εξής:

[1] Καθαρή κατάσταση (pure state) είναι μια κατάσταση ενός συστήματος την οποία γνωρίζουμε με ακρίβεια (π.χ. $|0\rangle, |1\rangle, |+\rangle, |-\rangle$).
Αντίθετα, μεικτή κατάσταση (mixed state) είναι μια κατάσταση την οποία δεν μπορούμε να γνωρίζουμε με ακρίβεια. Έτσι, την εκφράζουμε ως έναν πιθανοτικό συνδυασμό καθαρών καταστάσεων.
Στην σφαίρα του Bloch, οι καθαρές καταστάσεις ενός συστήματος που αποτελείται από 1 qubit περιγράφονται από σημεία στην επιφένεια, ενώ οι μεικτές από σημεία στο εσωτερικό της σφαίρας [8].

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \rightarrow \sum_i p_i U|\psi_i\rangle\langle\psi_i|U^t = U\rho U^t \text{ [10]}$$

Επίσης, στην γλώσσα του τελεστή πυκνότητας μπορούν να εκφραστούν και οι μετρήσεις. Αν εκτελέσουμε μια μέτρηση που περιγράφεται από τους τελεστές μέτρησης M_m σε μια αρχική κατάσταση $|\psi_i\rangle$, τότε η πιθανότητα να πάρουμε το αποτέλεσμα m είναι:

$$p(m|i) = \langle\psi_i|M_m^t M_m|\psi_i\rangle = tr(M_m^t M_m|\psi_i\rangle\langle\psi_i|) \text{ [10]}$$

Και συνολική πιθανότητα να πάρουμε το αποτέλεσμα m είναι:

$$p(m) = \sum_i p(m|i)p_i = tr(M_m^t M_m \rho)^{\,2} \text{ [10]}$$

Η συνολική κατάσταση του συστήματος αφού έχουμε πάρει το αποτέλεσμα m είναι:

$$|\psi_i^m\rangle = \frac{M_m|\psi_i^m\rangle}{\sqrt{\langle\psi_i|M_m^t M_m|\psi_i\rangle}} \text{ [10]}$$

Ο αντίστοιχος τελεστής πυκνότητας είναι:

$$\rho_m = \sum_i p(i|m)|\psi_i^m\rangle\langle\psi_i^m| = \sum_i p(i|m)\frac{M_m|\psi_i\rangle\langle\psi_i|M_m^t}{\langle\psi_i|M_m^t M_m|\psi_i\rangle} = \frac{M_m \rho M_m^t}{tr(M_m^t M_m \rho)} \text{ [10]}$$

2.13 Πιστότητα (Fidelity)

Η πιστότητα είναι ένας τρόπος μέτρησης απόστασης μεταξύ κβαντικών καταστάσεων.

Δωσμένων δύο καταστάσεων ρ,σ η πιστότητα είναι:

$$F(\rho, \sigma) = tr\left(\sqrt{\rho^{\frac{1}{2}}\sigma\rho^{\frac{1}{2}}}\right)$$

Η πιστότητα μεταξύ μιας καθαρής κατάστασης $|\psi\rangle$ και μιας τυχαίας κατάστασης ρ είναι:

$$F(|\psi\rangle, \rho) = \sqrt{\langle\psi|\rho|\psi\rangle} \text{ [8]}$$

2.14 Η Αρχή της Αβεβαιότητας του Heisenberg (Heisenberg's Uncertainty Principle)

Η αρχή της αβεβαιότητας του Heisenberg δηλώνει ότι εάν προετοιμάσουμε ένα μεγάλο αριθμό κβαντικών συστημάτων σε πανομοιότυπες καταστάσεις $|\psi\rangle$, και έπειτα εκτελέσουμε μετρήσεις

[2] tr είναι το ίχνος ενός πίνακα και ορίζεται ως το άθροισμα των διαγώνιων στοιχείων του: $tr(A) = \sum_i A_{ii}$.Για έναν διάνυσμα κατάστασης $|\psi\rangle$ και έναν τυχαίο τελεστή Α ισχύει: $tr(A|\psi\rangle\langle\psi|) = \langle\psi|A|\psi\rangle$ [8].

του παρατηρήσιμου C σε κάποια από αυτά τα συστήματα και μετρήσεις του D σε κάποια άλλα, τότε η τυπική απόκλιση του αποτελέσματος της μέτρησης του C (Δ(C)) επί την τυπική απόκλιση του αποτελέσματος της μέτρησης του D (Δ(D)) θα ικανοποιεί την εξίσωση:

$$\Delta(C)\Delta(D) \geq \frac{|\langle\psi|[C,D]|\psi\rangle|}{2} \text{ [8]}$$

2.15 Το EPR Παράδοξο (Einstein – Podolsky – Rosen Paradox)

Με την Κβαντική Διεμπλοκή, την οποία αναφέραμε ήδη, προκύπτει ένα μεγάλο παράδοξο, ωστόσο, το λεγόμενο EPR (Einstein–Podolsky–Rosen) paradox, το οποίο προτάθηκε από τους φυσικούς από τους οποίους πήρε το όνομά του, και αμφισβητεί την πληρότητα της εξήγησης της κβαντομηχανικής μέσα από την ερμηνεία της Κοπεγχάγης, η οποία είναι η ευρέως διαδεδομένη και αποδεκτή, έως και σήμερα. Το παράδοξο παρουσιάστηκε σε ένα άρθρο στις 25 Μαρτίου 1935 [10].

Η ερμηνεία της Κοπεγχάγης είναι αυτή που δηλώνει ότι τα φυσικά συστήματα δεν έχουν καθορισμένες ιδιότητες μέχρι να μετρηθούν, και τα αποτελέσματα τα οποία μπορούμε να πάρουμε από τους νόμους της Κβαντομηχανικής μπορούν να προβλέψουν μόνο τις πιθανότητες κατανομής των αποτελεσμάτων μιας μέτρησης. Επίσης, η πράξη της μέτρησης προκαλεί κατάρρευση της κυματοσυνάρτησης, κατά την οποία το σύνολο των πιθανοτήτων μειώνεται σε μόνο ένα εκ των πιθανών αποτελεσμάτων της μέτρησης, αμέσως μετά από αυτήν [10].

Το EPR παράδοξο είναι ένα νοητικό πείραμα κατά το οποίο δύο κβαντικά διαπλεγμένα σωματίδια βρίσκονται σε πάρα πολύ μεγάλη απόσταση μεταξύ τους, όταν η κυματοσυνάρτηση του ενός καταρρέει, λόγω μέτρησης, σε μία εκ των δύο βασικών καταστάσεων.
Τότε ταυτόχρονα, λόγω της κβαντικής διεμπλοκής, το άλλο σωματίδιο θα βρίσκεται στην αντίθετη βασική κατάσταση, ειδάλως θα παραβιαζώταν η αρχή αβεβαιότητας του Heisenberg. Όμως αυτό συνεπάγεται ότι, κάποια πληροφορία/σήμα, συγκεκριμένα η πληροφορία ότι το ένα σωματίδιο βρίσκεται πλέον στην x βασική κατάσταση, μεταφέρεται στιγμιαία , δηλαδή ταχύτερα και από την ταχύτητα του φωτός, στο άλλο σωματίδιο, και έτσι αυτό γνωρίζει και καταρρέει πάντα στην αντίθετη βασική κατάσταση (το γνωστό “spooky action at a distance”).

Όμως η θεωρία της σχετικότητας του Einstein απαγορεύει οποιοδήποτε αντικείμενο με μάζα να ταξιδεύει με ταχύτητα μεγαλύτερη ή ίση με την ταχύτητα του φωτός, καθώς θα απαιτούσε άπειρη ενέργεια για να το κάνει [10].

2.16 Ανισότητα του Bell.

Μέχρι στιγμής παρατηρούμε ότι στην Κβαντομηχανική επικρατεί μια «τυχαιότητα» (η λέξη τυχαιότητα μπαίνει σε παρένθεση καθώς η ερμηνεία της είναι περίπλοκη, και ελλοχεύουν μέχρι και φιλοσοφικοί προβληματισμοί κατά την χρήση της) και μια επικράτηση των πιθανοτήτων και της αβεβαιότητας. Αυτό αντιτίθεται σίγουρα στις εμπειρίες μας από τον καθημερινό κόσμο και δικαιολογημένα μας ξενίζει. Μήπως υπάρχουν κάποιες «κρυμμένες μεταβλητές», τις οποίες ακόμη δεν έχουμε ανακαλύψει και θα έλυναν αυτό το πρόβλημα; Κάποιες μεταβλητές οι οποίες ήταν ενσωματωμένες στα διαπλεγμένα σωματίδια, από την στιγμή που δημιουργήθηκαν; Μεταβλητές τις οποίες, εάν γνωρίζαμε, όλα τα φαινόμενα (συμπεριλαμβανομένις και των κβαντικών) θα ήταν ντετερμινιστικά και προβλεπτά; Αυτό είναι που υποστήριζαν οι Einstein, Podolsky, Rosen με το άρθρο τους το 1935 [10].

Οι Einstein, Podolsky, Rose ήταν υποστηρικτές του Τοπικού Ρεαλισμού (Local Realism), ο οποίος πρεσβεύει ότι κάθε σωματίδιο επηρεάζεται κατευθείαν μόνο από το άμεσο περιβάλλον του (Local) και κάθε κβαντική κατάσταση έχει σαφώς καθορισμένες ιδιότητες, ανεξαρτήτως από την πράξη της μέτρησης (Realism), δηλαδή ότι η πραγματικότητα υπάρχει, ανεξαρτήτως του αν κάνουμε κάποια μέτρηση σε αυτήν. Η Κβαντομηχανική, επέμειναν, ήταν μια ατελής θεωρία [8].

Ο N. Bohr (13 Ιουλίου 1935), με καινούριο άρθρο με τον ίδιο ακριβώς τίτλο, υποστήριξε το αντίθετο, δηλαδή την θεωρία της Κοπεγχάγης, επισημαίνοντας ότι είναι ανούσιο να αναθέσουμε πραγματικότητα στο σύμπαν, υπό την απουσία παρατήρησης. Τα κβαντικά συστήματα στα χρονικά διαστήματα μεταξύ μετρήσεων, υπάρχουν μόνο ως ασαφή μείγματα όλων των πιθανών ιδιοτήτων (superposition of states). Η εμπειρία μας ενός καλώς ορισμένου, υλικού σύμπαντος έχει νόημα μόνο κατά τη διάρκεια της μέτρησης [11].

Ο Ιρλανδός φυσικός John Bell με το άρθρο “On the Einstein Podolsky Rosen Paradox”, το 1964 πρότεινε ένα πείραμα για να επιλύσει τη διαμάχη των Bohr-Einstein, το οποίο ήταν

περισσότερο φιλοσοφικό μέχρι εκείνη την στιγμή. Απέδειξε ότι καμιά θεωρία κρυμμένων μεταβλητών που διατηρεί τις παραδοχές της τοπικότητας και του ντετερμινισμού δεν μπορεί να πετύχει τις προβλέψεις της κβαντικής φυσικής, μέσω ενώς νοητικού πειράματος, το οποίο στην συνέχεια υλοποιήθηκε και στον φυσικό κόσμο [8].

Η περιγραφή του πειράματος έχει ως εξής:
Έχουμε ένα διαπλεγμένο ζευγάρι (ή ζεύγος διεμπλοκής, ή ζευγάρι σε κατάσταση διεμπλοκής, όλα έχουν την ίδια σημασία) ηλεκτρονίου-ποζιτρονίου, τα οποία έχουν πάντα αντίθετα spin, βέβαια δεν μπορούμε να ξέρουμε προς τα ποια διεύθυνση, μέχρι να κάνουμε κάποια μέτρηση σε ένα εκ των δύο.
Η απάντηση στο πώς επηρεάζει η μέτρηση του ενός, το spin του διαπλεγμένου ζεύγους του, θα διευθετήσει τη διαμάχη [8].

Σενάριο 1: Εάν ο Einstein είχε δίκιο και υπήρχαν κρυμμένες μεταβλητές που καθορίζουν την αντίδραση του κάθε σωματιδίου σε κάθε πιθανή μέτρηση του spin του εξ' αρχής, ό,τι και να κάναμε αργότερα στο ένα σωματίδιο, δεν θα μπορούσε να επηρεάσει το άλλο. Έτσι, όταν μετρήσουμε τα spins των δύο σωματιδίων, θα υπάρχει κάποια συσχέτιση των αποτελεσμάτων, καθώς τα σωματίδια ήταν κάποτε συνδεδεμένα, αλλά δεν θα υπάρχει συσχέτιση λόγω της επιλογής μας για τον άξονα μέτρησης [8].

Σενάριο 2: Εάν ο Bohr είχε δίκιο, μεταξύ της δημιουργίας και της μέτρησης, το ηλεκτρόνιο και το ποζιτρόνιο υπάρχουν μόνο ως κυματοσυναρτήσεις όλων των πιθανών κβαντικών καταστάσεων. Σε αυτήν την περίπτωση η μέτρηση του ενός σωματιδίου θα προκαλούσε κατάρρευση της κυματοσυνάρτησής του, και θα έπαιρνε καθορισμένες τιμές. Τότε, και τα δύο σωματίδια θα παρουσιάσουν αντίθετα spins ως προς τον άξονα μέτρησης που επιλέξαμε για ένα εκ των δύο σωματιδίων. Αυτό θα οδηγήσει σε κάποια συσχέτιση μεταξύ του άξονα μέτρησης που επιλέξαμε για το πρώτο σωματίδιο και την διεύθυνση spin του δεύτερου [8].

Η ανισότητα του Bell είναι η εξής:

$$E(QS) + E(RS) + E(RT) - E(QT) \leq 2 \quad [8]$$

Αυτή, θα έπρεπε να ισχύει πάντα, σε περίπτωση που η ερμηνεία του Einstein (σενάριο 1) ήταν η σωστή. Ωστόσο, αν ένα πείραμα διεμπλοκής παραβίαζε αυτήν την συνθήκη, τότε η θεωρία του τοπικού ρεαλισμού παραβιάζεται επίσης, το οποίο διαψεύδει την αρχή της τοπικότητας ή/και η αρχή του ρεαλισμού [8].

(Δεν μπαίνουμε σε λεπτομέρειες του πειράματος καθώς είναι πολύ περίπλοκες και περιττές, μιας και σκοπεύουμε να εστιάσουμε μόνο στα απαραίτητα και να θέσουμε την φυσική βάση για να ασχοληθούμε με τους κβαντικούς υπολογιστές.)

Το αποτέλεσμα ήταν να παραβιάζεται η εξίσωση του Bell, και άρα κατέστησε την ερμηνεία του Einstein λανθασμένη οριστικά, και σκότωσε την οποιαδήποτε ελπίδα για «κρυφές μεταβλητές» [8].

ΚΕΦΑΛΑΙΟ 3

Εισαγωγή στην κβαντική υπολογιστική

3.1 Κβαντικό Bit (Qubit)

Οι κλασσικοί υπολογιστές απεικονίζουν όλη την πληροφορία με τα γνωστά σε όλους μας δυαδικά ψηφία ή bits, με τιμές 0 ή 1. Στους κβαντικούς υπολογιστές το αντίστοιχο γίνεται με τα quantum bits (qubits), με τις δύο καταστάσεις $|0\rangle$ και $|1\rangle$, οι οποίες είναι γνωστές και ως καταστάσεις υπολογιστικής βάσης (computation basis states ή CBS) [8,9].

Σε αντίθεση με τους κλασσικούς υπολογιστές, στους κβαντικούς υπολογιστές ένα qubit μπορεί να βρίσκεται ταυτόχρονα στις καταστάσεις $|0\rangle$ και $|1\rangle$, να βρίσκεται, δηλαδή, σε κβαντική υπέρθεση (quantum superposition). Ωστόσο, από την στιγμή που θα πραγματοποιήσουμε μία μέτρηση, η κβαντική κατάσταση του qubit θα καταρρεύσει και θα επιστρέψει σε μία εκ των δύο βασικών καταστάσεων $|0\rangle$ και $|1\rangle$ [8,9].

Πολλά κβαντικά συστήματα δύο καταστάσεων μπορούν να χρησιμοποιηθούν ως qubit, με πιο γνωστά παραδείγματα την πόλωση ενός φωτονίου, και το spin ενός ηλεκτρονίου [8,9].

Η αρχική κατάσταση ενός qubit είναι πάντα μία από τις δύο βασικές του καταστάσεις και στην συνέχεια, με διαδοχική εφαρμογή κβαντικών πυλών, μπορούμε να έχουμε κβαντική υπέρθεση διαφόρων καταστάσεων $|\psi\rangle = a|0\rangle + \beta|1\rangle$. Μετά την μέτρηση η πιθανότητα το qubit να βρίσκεται στην κατάσταση $|0\rangle$ είναι $|\alpha|^2$, ενώ η πιθανότητα να βρίσκεται στην κατάσταση $|1\rangle$, είναι $|\beta|^2$, όπου α,β είναι μιγαδικοί αριθμοί, και η συνολική πιθανότητα το σύστημα να βρίσκεται σε μία εκ των δύο καταστάσεων αθροίζει στο 1 (η κατάσταση ενός qubit πρέπει να είναι κανονικοποιημένη στο 1). Με την μέτρηση, το σύστημά μας θα επιστρέψει σε μία εκ των δύο βασικών καταστάσεων [8,9].

Για παράδειγμα, το qubit μας, μπορεί να βρίσκεταις την κατάσταση:

$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$,

Το οποίο όταν μετρηθεί, θα δώσει $|0\rangle$, $\left(\frac{1}{\sqrt{2}}\right)^2$ των φορών, και $|1\rangle$, $\left(\frac{1}{\sqrt{2}}\right)^2$ των φορών [8,9].

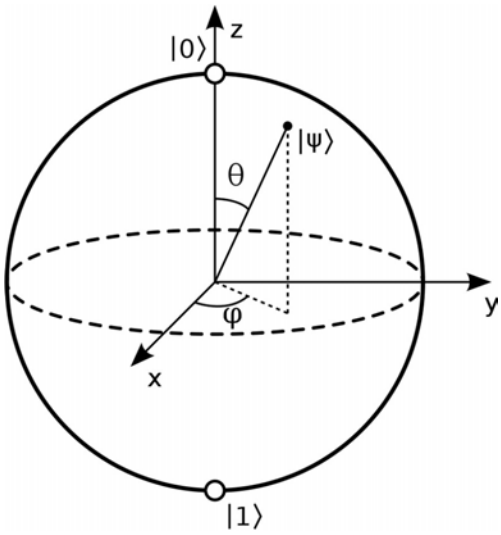
Προφανώς η μνήμη ενός κβαντικού υπολογιστή δεν θα αποτελείται από ένα μόνο qubit, αλλά από έναν μεγάλο αριθμό αυτών, τοποθετημένα κοντά, αλλά όχι πολύ κοντά, ώστε να είναι δυνατός ο ανεξάρτητος «έλεγχός» τους με κατάλληλα εξωτερικά πεδία [8].

3.2 Σφαίρα Bloch (Bloch Sphere)

Μπορούμε να εκφράσουμε την κατάσταση ενός qubit και ως:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle \ \ [8]$$

Οι αριθμοί θ,φ ορίζουν ένα σημείο στην τρισδιάστατη μοναδιαία σφαίρα. Αυτή η σφαίρα, η οποία αναπαριστά τον χώρο καταστάσεων ενός κβαντικού συστήματος ενός qubit, λέγεται και Bloch Sphere [8].



Εικόνα 3.1: Η σφαίρα Bloch [8].

3.3 Καταστάσεις 2 qubit

Από πού πηγάζει όμως η τεράστια υπολογιστική ισχύς ενός κβαντικού υπολογιστή;

Ας πάρουμε, για παράδειγμα την περίπτωση του κβαντικού υπολογιστή με 2 qubit. Οι δυνατές καταστάσεις του συστήματος προκύπτουν από το Kronecker Product των 2 qubit και είναι οι :

$$|00\rangle = |0\rangle \otimes |0\rangle,$$
$$|01\rangle = |0\rangle \otimes |1\rangle,$$
$$|10\rangle = |1\rangle \otimes |0\rangle,$$

$$|11\rangle = |1\rangle \otimes |1\rangle,$$

Αυτές, αποτελούν μια υπολογιστική βάση στον τετρασδιάστατο χώρο των 2 qubit.
Τώρα, η κάθε κβαντική κατάσταση περιγράφεται από την επαλληλία:

$|\Psi\rangle = |\mathrm{a}\rangle \otimes |\mathrm{b}\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$, όπου $|\mathrm{a}\rangle, |b\rangle$ *είναι τα* 2 *αρχικά qubit*

Το αποτέλεσμα τώρα της μέτρησης, δηλαδή $|00\rangle$ ή $|01\rangle$ ή $|10\rangle$ ή $|11\rangle$, προκύπτει με αντίστοιχες πιθανότητες $|\alpha|^2$ ή $|\beta|^2$ ή $|\gamma|^2$ ή $|\delta|^2$, με την συνθήκη κανονικοποίησης να επιβάλει ότι: $|\alpha|^2 + |\beta|^2 + |\gamma|^2 + |\delta|^2 = 1$.

Εύκολα μπορούμε να γενικεύσουμε τα παραπάνω για πολλά qubits με πιθανά αποτελέσματα $|x\rangle$, με πιθανότητα $|\alpha_x|^2$ και συνθήκη κανονικοποίησης $\sum_x |a_x|^2 = 1$ [8].

Έτσι, παρατηρούμε ότι με μόλις 2 qubit, αναπαραστήσαμε ένα 4-D διάνυσμα, ή αλλιώς, την επαλληλία 4 βασικών καταστάσεων. Γενικότερα η σχέση δείχνει ότι με n qubits, μπορούμε να παράγουμε ένα διάνυσμα στον 2^n χώρο. Αυτό σημαίνει ότι με 200 qubits, θα μπορούσαμε να αναπαραστίσουμε τον γραμμικό συνδυασμό $\sim 10^{87}$βασικών καταστάσεων.

Βέβαια ας μην ενθουσιαζόμαστε υπερβολικά, καθώς κάτι τέτοιο στην πράξη, απέχει πολύ ακόμη. Τα qubits είναι πάρα πολύ ευαίσθητα στον θόρυβο του περιβάλλοντος, και όσο περισσότερα αποτελούν το κβαντικό μας σύστημα, τόσο δυσκολότερο γίνεται να διατηρηθεί στην κατάστασή του και να μην καταρρεύσει. Πρέπει να κατανοήσουμε και να μάθουμε να ελέγχουμε αυτές τις ανεπιθύμητες αλληλεπιδράσεις με το περιβάλλον, ώστε να κατασκευάσουμε αξιόπιστα εργαλεία επεξεργασίας κβαντικής πληροφορίας (περισσότεροι προβληματισμοί στο κεφάλαιο 7).

3.4 Κβαντικός Καταχωρητής (Quantum Register)

Το αντίστοιχο τον κλασσικών καταχωρητών στους κλασσικούς υπολογιστές, είναι οι κβαντικοί καταχωρητές στους κβαντικούς υπολογιστές. Αυτήν την φορά, αντί να αποθηκεύουν τις τιμές μεταβλητών με τη μορφή συνόλων από bits, αποθηκεύουν σύνολα από qubits, τα οποία περιγράφουν κάποια κβαντική κατάσταση [9].

Η κατάσταση ενός κβαντικού καταχωρητή είναι το τανυστικό γινόμενο των καταστάσεων των qubits που τον αποτελούνε:

$|q_R\rangle = |q_1\rangle \otimes |q_2\rangle = |q_1\rangle|q_2\rangle = |q_1, q_2\rangle = |q_1\ q_2\rangle$ [9]

Έτσι, για παράδειγμα, η κβαντική κατάσταση ενός καταχωρητή 3 qubit μπορεί να είναι η:

$$|q_R\rangle = |q_1\rangle \otimes |q_2\rangle \otimes |q_3\rangle = |1\rangle \otimes |1\rangle \otimes |0\rangle = |110\rangle = \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\\1\end{bmatrix} \otimes \begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}0\\0\\0\\0\\0\\0\\1\\0\end{bmatrix}$$

$$= 0 * |000\rangle + 0 * |001\rangle + 0 * |010\rangle + 0 * |011\rangle + 0 * |100\rangle + 0 * |101\rangle + 1 * |110\rangle + 0 * |111\rangle$$

Όπου οι συντελεστές των βασικών καταστάσεων του συστήματος μας είναι τα πλάτη πιθανότητας (probability amplitudes).

Στην γενική περίπτωση έχουμε 2^nπλάτη πιθανότητας, όπου n είναι ο αριθμός qubit, για τα οποία ισχύει ότι το άθροισμα των τετραγώνων τους είναι πάντα 1. Το διάνυσμα κατάστασης στην γενική περίπτωση βρίσκεται στον μιγαδικό χώρο Hilbert 2^n διαστάσεων, με 2^n βασικές καταστάσεις, ορθογώνιες μεταξύ τους.

Στο παράδειγμα που παρουσιάσαμε ο καταχωρητής 3 qubit βρίσκεται σε μία εκ των βασικών καταστάσεων. Στην γενική περίπτωση, ο καταχωρητής μπορεί να βρίσκεται σε μια υπέρθεση όλων των βασικών καταστάσεων του χώρου Hilbert στον οποίο ανήκει το διάνυσμα που περιγράφει την κατάσταση μας:

$$|q_R\rangle = c_0 * |0 \dots 00\rangle + c_1 * |0 \dots 01\rangle + \cdots + c_{2^n-1} * |1 \dots 11\rangle$$ [9]

Πάνω σε αυτήν την ιδιότητα της υπέρθεσης βασίζεται η τεράστια υπολογιστικής ισχύς των κβαντικών υπολογιστών [9].

3.5 Κβαντική Μέτρηση

Το ζήτημα της μέτρησης είναι το βασικό πρόβλημα της Κβαντομηχανικής. Όταν κάνουμε μια μέτρηση πάνω σε ένα κβαντικό σύστημα, η κυματομορφή του καταρρέει, με αποτέλεσμα η μέτρησή μας να μην δείχνει αυτό που αναζητούσαμε στην αρχή. Για παράδειγμα, όταν πάμε να μετρήσουμε ένα qubit, αυτό θα επιστρέψει σε μία εκ των δύο βασικών του καταστάσεων, $|0\rangle$ ή $|1\rangle$ [4,7].

Γιατί συμβαίνει αυτό, όμως;
Μια συχνή παρανόηση είναι ότι αυτό έχει να κάνει με την ύπαρξη ή όχι συνειδητού παρατηρητή, αλλά αυτό προφανώς είναι λάθος. Ο λόγος που συμβαίνει αυτό, είναι ότι τα συστήματα που υπακούν στους νόμους της κβαντικής φυσικής (π.χ. 1 qubit που μπορεί να είναι 1 φωτόνιο ή 1 ηλεκτρόνιο) είναι τόσο ελαφριά, που οποιαδήποτε μέτρηση επιχειρήσουμε να κάνουμε, μιας και η μέτρηση είναι μια φυσική πράξη και δεν γίνεται δια μαγείας (π.χ. όταν ρίχνουμε φως για να δούμε ένα αντικείμενο, στην ουσία το «λούζουμε» με φωτόνια), προκαλεί κάποια αλληλεπίδραση (σύγκρουση) αυτών των σωματιδίων, η οποία αλλάζει την κατάστασή τους, σύμφωνα με κάποια κατανομή πιθανότητας, η οποία περιγράφεται από τα μαθηματικά της κβαντικής φυσικής [4,7].

Μια κβαντική μέτρηση περιγράφεται από μια ορθοκανονική βάση $|e_j\rangle$ στον χώρο καταστάσεων. Αν η αρχική κατάσταση του συστήματος είναι $|\psi\rangle$, τότε παίρνουμε το αποτέλεσμα $|j\rangle$ με πιθανότητα:

$$Prob(j) = \left|\langle e_j|\psi\rangle\right|^2 \text{ [4]}$$

Και η μετέπειτα κατάσταση (a posterior state) είναι η $|e_j\rangle$ [4].

3.5.1 Προβολικές Μετρήσεις

Οι προβολικές μετρήσεις είναι μια ειδική περίπτωση των γενικών μετρήσεων. Σε πολλές εφαρμογές κβαντικού υπολογισμού ασχολούμαστε κυρίως με τις προβολικές μετρήσεις .

Μια προβολική μέτρηση περιγράφεται από ένα Παρατηρίσιμο, M, και έναν Ερμιτιανό Τελεστή στον χώρο καταστάσεων στον οποίο το σύστημα παρατηρείται [8]. Το Παρατηρήσιμο έχει φασματική ανάλυση :

$$M = \sum_m mP_m \text{ [8]}$$

Όπου:

- P_m είναι ο προβολέας στον ιδιοχώρο (eigenspace) του M με ιδιοτιμή m

Τα πιθανά αποτελέσματα μιας μέτρησης αντιστοιχούν στις ιδιοτιμές m του Παρατηρήσιμου. Με την μέτρηση της κατάστασης $|\psi\rangle$, η πιθανότητα να πάρεις αποτέλεσμα m είναι:

$$p(m) = \langle\psi|P_m|\psi\rangle \text{ [8]}$$

Αν πάρουμε ως αποτέλεσμα την ιδιοτιμή m, η μετέπειτα κατάσταση (a posterior state) του συστήματος είναι η:

$$\frac{P_m(\psi)}{\sqrt{p(m)}} \text{ [8]}$$

Η μέση τιμή της μέτρησης του συστήματος είναι:

$$E(M) = \langle M\rangle = \langle\psi|M|\psi\rangle \text{ [8]}$$

Και η τυπική απόκλιση των μετρήσεων:

$$[\Delta(M)]^2 = \langle M^2\rangle - \langle M\rangle^2, \text{ [8]}$$

η οποία δηλώνει την παρατηρήσιμη εξάπλωση των παρατηρήσιμων τιμών μετά την μέτρηση του M [8].

3.5.2 Μερικές Μετρήσεις

Τα πράγματα είναι πολύ απλά όταν θέλουμε να μετρήσουμε μόνο 1 qubit ή ένα ενιαίο σύνολο από qubits. Τι συμβαίνει όμως όταν θέλουμε να μετρήσουμε μόνο μερικά από τα qubit τα οποία αποτελούν το κβαντικό σύστημά μας;

Αν, για παράδειγμα, έχουμε ένα σύστημα από 2 qubits, $\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$ και κάνουμε μέτρηση μόνο στο πρώτο qubit, ποιες είναι οι πιθανότητες να πάρουμε $|0\rangle$ ή $|1\rangle$ ως τιμή αυτού του qubit; Ποια είναι η κατάσταση του συστήματος αφού έχει γίνει η μέτρηση (posterior state);

Η πιθανότητα υπολογίζεται ως εξής:

$$Prob(0) = Prob(00) + Prob(01) = |\alpha|^2 + |\beta|^2$$

$$Prob(1) = Prob(10) + Prob(11) = |\gamma|^2 + |\delta|^2$$

$$\text{Γενικά: } \text{Prob}(0 \text{ ή } 1) = \sum_m |\alpha_m|^2 \quad [8]$$

Όπου:

- α_m είναι όλα τα πλάτη πιθανότητας του συστήματος όπου το qubit που μετράμε έχει την τιμή $|0\rangle$ ή $|1\rangle$.

Και το a posterior state, αν μετά την μέτρηση το πρώτο qubit είναι $|0\rangle$:

$$|\psi\rangle = \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle = |0\rangle(\alpha|0\rangle + \beta|1\rangle) + |1\rangle(\gamma|0\rangle + \delta|1\rangle)$$

$$|\psi'\rangle = |0\rangle \otimes \frac{\alpha|0\rangle + \beta|1\rangle}{\sqrt{\alpha^2 + \beta^2}}$$

$$\text{Γενικά: } |\psi'\rangle = |0 \text{ ή } 1\rangle \otimes \frac{\sum_m |\alpha_m||m\rangle}{\sqrt{\sum_m |\alpha_m|^2}} \quad [8]$$

3.5.3 Μερικές Μετρήσεις σε Αυθαίρετη Βάση

Τι θα συναίβαινε όμως αν, αντί για μετρήσεις στην υπολογιστική βάση $|0\rangle$, $|1\rangle$ κάναμε τις μετρήσεις σε μια αυθαίρετη ορθοκανονική βάση $|e_0\rangle$, $|e_1\rangle$, όπου για παράδειγμα:

$$|e_0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, |e_1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Εκφράζουμε το πρώτο qubit στην υπάρχουσα κατάσταση συναρτήσει της νέας βάσης μας και προκύπτουν καινούριοι συντελεστές, οι οποίοι είναι συναρτήσεις των παλιών συντελεστών:

$$|\psi'\rangle = \alpha'|e_0 0\rangle + \beta'|e_0 1\rangle + \gamma'|e_1 0\rangle + \delta'|e_1 1\rangle$$

Τότε, η πιθανότητα και η μετέπειτα κατάσταση του συστήματος είναι αντίστοιχα:

$$Prob(e_0) = Prob(e_0 0) + Prob(e_0 1) = |\alpha'|^2 + |\beta'|^2$$

$$|\psi'\rangle = |e_0\rangle \otimes \frac{\alpha'|0\rangle + \beta'|1\rangle}{\sqrt{\alpha'^2 + \beta'^2}}$$

Παρατηρούμε επίσης ότι:

$$|0\rangle = \frac{|e_0\rangle + |e_1\rangle}{\sqrt{2}}, |1\rangle = \frac{|e_0\rangle - |e_1\rangle}{\sqrt{2}}$$

‘Ετσι μπορούμε να εκφράσουμε την αρχική μας κατάσταση ως:

$$\begin{aligned} |\psi\rangle &= \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle \\ &= \frac{\alpha+\gamma}{\sqrt{2}}|e_0 0\rangle + \frac{\beta+\delta}{\sqrt{2}}|e_0 1\rangle + \frac{\alpha-\gamma}{\sqrt{2}}|e_1 0\rangle + \frac{\beta-\delta}{\sqrt{2}}|e_1 1\rangle \end{aligned}$$

Και την πιθανότητα και την μετέπειτα κατάσταση:

$$Prob(e_0) = \frac{|\alpha+\gamma|^2 + |\beta+\delta|^2}{2}$$

$$|\psi'\rangle = |e_0\rangle \otimes \frac{(\alpha+\gamma)|0\rangle + (\beta+\delta)|1\rangle}{\sqrt{|\alpha+\gamma|^2 + |\beta+\delta|^2}}$$

Σε γενικές, πιο περίπλοκες καταστάσεις, όπου έχουμε σύστημα πολλών qubit σε αυθαίρετη βάση και θέλουμε να μετρήσουμε τα πρώτα j qubits:

Μετράμε τα πρώτα j qubits, τα οποία βρίσκονται στην κατάσταση:

$$\sum_{jk} a_{jk} |e_j\rangle |k\rangle$$

Η πιθανότητα να πάρεις ως αποτέλεσμα το e_j, μετρώντας στην ορθοκανονική βάση $\sum_j |e_j\rangle$ είναι:

$$Prob(e_j) = \sum_k |a_{jk}|^2$$

Και η μετέπειτα κατάσταση:

$$|\psi'\rangle = |e_j\rangle \otimes \sum_k \frac{\alpha_{jk}|k\rangle}{\sqrt{\sum_k |a_{jk}|^2}}$$

Όπου:

- a_{jk} είναι τα πλάτη πιθανότητας της νέας κατάστασης
- $|e_j\rangle$ είναι η ορθοκανονική βάση στην οποία μετράμε το πρώτο qubit
- $|k\rangle$ είναι η υπολογιστική βάση στην οποία εκφράζονται τα υπόλοιπα qubits

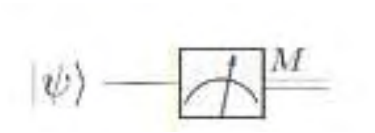
Οι μερικές μετρήσεις σε αυθαίρετη βάση είναι πολύ σημαντικές για τον αλγόριθμο της Κβαντικής Τηλεμεταφοράς [8].

3.6 Κβαντικά Κυκλώματα (Quantum Circuits)

Τα κβαντικά κυκλώματα στην κβαντική θεωρία πληροφορίας είναι τα αντίστοιχα των αναλογικών κυκλωμάτων της κλασσικής θεωρίας πληροφορίας. Πρόκειται για μια αναπαράσταση ενός συστήματος κβαντικού υπολογισμού ως μια αλληλουχία κβαντικών πυλών, οι οποίες είναι πάντα αντιστρέψιμοι μετασχηματισμοί, οι οποίες εφαρμόζονται σε έναν κβαντικό καταχωρητή μεγέθους n qubit. Πολύ συχνά η κατάσταση εισόδου σε ένα κβαντικό κύκλωμα είναι ο n-qubit καταχωρητής που αποτελείται μόνο από $|0\rangle$ [8].

Οι γραμμές στο κύκλωμα αναπαριστούν, όπως και σε ένα κλασσικό κύκλωμα, τα κβαντικά «καλώδια», τα οποία χρησιμοποιούνται ως μέσο για να μεταφερθεί η πληροφορία. Τα «καλώδια» σε ένα κβαντικό κύκλωμα δεν έχουν αναγκαστικά τη μορφή των φυσικών καλωδίων που έχουμε συνηθίσει από την καθημερινότητά μας. Έχουν μια πιο αυθαίρετη σημασία, ανάλογα και με το κάθε κύκλωμα. Μπορεί να απεικονίζουν το πέρασμα του χρόνου, ή τη μετάδοση ενός φωτονίου από ένα σημείο του χώρου σε ένα άλλο [8].

Αξίζει να σημειώσουμε ότι η διαδικασία της μέτρησης, την οποία έχουμε ήδη αναλύσει παραπάνω, σε ένα κβαντικό κύκλωμα απεικονίζεται με το εξής σχήμα:



Εικόνα 3.2: Συμβολισμός μέτρησης σε ένα κβαντικό κύκλωμα [8].

Τα κβαντικά κυκλώματα έχουν κάποιες πολύ βασικές διαφορές από τα κλασσικά κυκλώματα.

- Τα κβαντικά κυκλώματα δεν επιτρέπουν βρόχους.
- Τα κβαντικά κυκλώματα δεν επιτρέπουν την ένωση καλωδίων, η οποία θα παρήγαγε το αποτέλεσμα της λογικής πράξης OR, η οποία είναι μη αντιστρέψιμη.
- Τα κβαντικά κυκλώματα απαγορεύουν την αντιγραφή ενός qubit [8].

3.6.1 Κύκλωμα ανταλλαγής (SWAP)

Ένα παράδειγμα ενός πολύ γνωστού, μικρού, απλού και χρήσιμου, όπως θα δούμε παρακάτων, κβαντικούς κυκλώματος είναι το κύκλωμα ανταλλαγής qubit (SWAP).

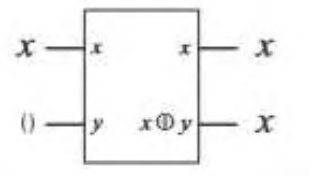
Εικόνα 3.3: Το κύκλωμα ανταλλαγής [8].

Εδώ βλέπουμε δύο ισοδύναμους τρόπου να απεικονίσουμε το κύκλωμα ανταλλαγής.
Το γιατί αυτό το κύκλωμα στην ουσία ανταλλάσσει τις τιμές δύο qubit μπορούμε να το δούμε εάν ακολουθίσουμε πιστά την αλληλουχία πράξεων που συμβολίζει το σχήμα της αριστερά εικόνας:

$|a,b\rangle \rightarrow |a,a\oplus b\rangle \rightarrow |a\oplus(a\oplus b),a\oplus b\rangle = |b,a\oplus b\rangle \rightarrow |b,(a\oplus b)\oplus b\rangle \rightarrow |b,a\rangle$ [8]

3.6.2 Κύκλωμα αντιγραφής qubit (qubit-copying circuit)

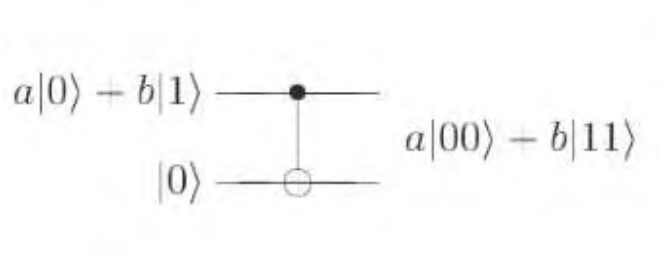
Η αντιγραφή ενός bit άγνωστης τιμής σε ένα κλασσικό κύκλωμα γίνεται πολύ εύκολα με την χρήση μιας CNOT πύλης:



Εικόνα 3.4: Κλασσικό κύκλωμα αντιγραφής bit [8].

Το να κάνουμε το ίδιο σε ένα κβαντικό κύκλωμα αποδεικνύεται όχι τόσο εύκολο. Για την ακρίβεια, αποδεικνύεται αδύνατο [8].

Το αντίστοιχο κβαντικό κύκλωμα με το κλασσικό που δείξαμε παραπάνω είναι το εξής:



Εικόνα 3.5: Απόπειρα αντιγραφής qubit με κβαντικό κύκλωμα [8].

Η λειτουργία της C-NOT πύλης είναι να αντιστρέψει το δεύτερο qubit (target qubit) σε περίπτωση που το πρώτο (control qubit) είναι 1 (θα την αναλύσουμε στο *3.9.1*).

- Έστω ότι το control qubit μας βρίσκεται στην γενική κατάσταση $|\psi\rangle = a|0\rangle + b|1\rangle$.
- Η αρχική μας κατάσταση είναι η $|\psi\rangle|0\rangle = [a|0\rangle + b|1\rangle]|0\rangle = a|00\rangle + b|10\rangle$.
- Μετά την εφαρμογή της C-NOT η κατάστασή μας γίνεται η $a|00\rangle + b|11\rangle$.
- Είναι αυτή η κατάσταση η ίδια με την κατάσταση $|\psi\rangle|\psi\rangle$;
  Όχι, καθώς $|\psi\rangle|\psi\rangle = a^2|00\rangle + ab|01\rangle + ba|10\rangle + b^2|11\rangle$.
  Η μόνη περίπτωση για την οποία ισχύει αυτό, είναι όταν η αρχική μας κατάσταση $|\psi\rangle$ είναι η κατάσταση $|0\rangle$ ή $|1\rangle$ [8].

3.6.3 Θεώρημα μη-κλωνοποίησης (no-cloning theorem)

Το θεώρημα μη-κλωνοποίησης αποδεικνύει ότι είναι αδύνατο να κάνουμε ένα αντίγραφο μια προηγουμένως άγνωστης κβαντικής κατάστασης:

❖ Έστω ότι έχουμε μια κβαντική μηχανή η οποία έχει δύο θέσης A, B.
  Η θέση A είναι είναι η θέση δεδομένων (data slot) και η θέση B η θέση στόχου (target slot).
  Επιθυμούμε να αντιγράψουμε ότι περιέχεται στη θέση A στη θέση B.
  Η αρχική κατάσταση του data slot είναι μια άγνωστη καθαρή κατάσταση $|\psi\rangle$.
  Η αρχική κατάσταση του target slot είναι μια σταθερή καθαρή κατάσταση $|s\rangle$.
  Η αρχική κατάσταση του συστήματός μας είναι :

$$|\psi\rangle \otimes |s\rangle$$

- Τώρα λαμβάνει χώρα ο μετασχηματισμός U, οποίος είναι ο μετασχηματισμός που πραγματοποιεί την αντιγραφή του άγνωστου qubit. Ιδανικά, η λειτουργία του είναι η εξής:

$$|\psi\rangle \otimes |s\rangle \xrightarrow{U} U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

- Έστω τώρα ότι εφαρμόζουμε τον εξής μετασχηματισμό σε δύο διαφορετικές καταστάσεις $|\psi\rangle, |\varphi\rangle$:

$$U(|\psi\rangle \otimes |s\rangle) = |\psi\rangle \otimes |\psi\rangle$$

$$U(|\varphi\rangle \otimes |s\rangle) = |\varphi\rangle \otimes |\varphi\rangle$$

- Το εσωτερικό γινόμενο των δύο αυτών εξισώσεων δίνει:

$$\langle\psi|\varphi\rangle = (\langle\psi|\varphi\rangle)^2$$

- Η μόνες περιπτώσεις που το παραπάνω ισχύει είναι εάν $\langle\psi|\varphi\rangle = 0$ ή $\langle\psi|\varphi\rangle = 1$. Άρα μόνο στην περίπτωση που τα $|\psi\rangle, |\varphi\rangle$ είναι ίδια ή ορθογώνια μεταξύ τους.

Επομένως μια κβαντική μηχανή κλωνοποίησης μπορεί να κλωνοποιήσει μόνο καταστάσεις οι οποίες είναι ορθογώνιες μεταξύ τους. Μια γενική μηχανή που δουλεύει σε όλες τις περιπτώσεις δεν μπορεί να δημιουργηθεί [8].

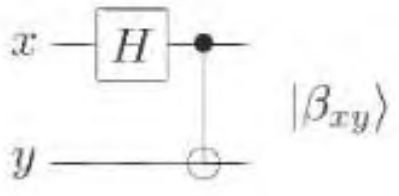
3.6.4 Κύκλωμα προετοιμασίας καταστάσεων Bell

Οι καταστάσεις Bell χρησιμοποιούνται πάρα πολύ συχνά στου κβαντικούς υπολογισμούς και είναι διαπλεγμένες καταστάσεις (στο 2.19 εξηγούμε τι είναι κβαντική διεμπλοκή) [8].

Αυτές, μαζί με το κύκλωμα που τις προετοιμάζει φαίνονται παρακάτω :

Πίνακας 3.1: Αριστερά: Καταστάσεις Bell

In	Out
$\|00\rangle$	$(\|00\rangle + \|11\rangle)/\sqrt{2} \equiv \|\beta_{00}\rangle$
$\|01\rangle$	$(\|01\rangle + \|10\rangle)/\sqrt{2} \equiv \|\beta_{01}\rangle$
$\|10\rangle$	$(\|00\rangle - \|11\rangle)/\sqrt{2} \equiv \|\beta_{10}\rangle$
$\|11\rangle$	$(\|01\rangle - \|10\rangle)/\sqrt{2} \equiv \|\beta_{11}\rangle$



Εικόνα 3.6: Δεξιά: Κύκλωμα προετοιμασίας των καταστάσεων Bell [8].

3.7 Κβαντικοί Αλγόριθμοι (Quantum Algorithms)

Με το κατάλληλο κβαντικό κύκλωμα, μπορούμε να αναπαραστήσουμε οποιοδήποτε κλασσικό λογικό κύκλωμα, πράγμα λογικό, αφού όλος ο κόσμος γύρω μας λειτουργεί με βάση τους κανόνες της Κβαντομηχανικής. Η κλασσική φυσική, είναι απλά μια οριακή κατάσταση της κβαντικής φυσικής [8].

Οι κβαντικοί αλγόριθμοι, οι οποίοι έχουν δημιουργηθεί αλλά και γίνονται προσπάθειες να δημιουργηθούν, όλοι λαμβάνουν υπ' όψιν αυτήν το πρόβλημα της μέτρησης. Δεν σχεδιάζονται με τον ίδιο τρόπο όπως οι κλασσικοί αλγόριθμοι. Η συνήθης διαδικασία που ακολουθούν είναι η εξής:

1. Προετοίμασε μια κβαντική κατάσταση κάποιων qubit.
2. Κάνε κάποιες ενέργεις (εφαρμογή τελεστών μέσω κβαντικών πυλών) πάνω σε αυτήν.
3. Κάνε κάποια μέτρηση στην κβαντική σου κατάσταση.
4. Επανέλαβε κάποιες φορές αυτήν την διαδικασία, ώστε να είσαι αρκετά βέβαιος για το αποτέλεσμά σου.

Το τέταρτο βήμα, είναι το ασυνήθιστο. Καθώς η μέτρηση που θα πάρουμε δίνει κάποιες καταστάσεις με τις αντίστοιχες πιθανότητές τους, πρέπει να επαναλάβουμε την διαδικασία κάποιες φορές, ώστε η πιθανότητα να έχουμε λάβει την σωστή απάντηση, δηλαδή αυτήν με την μεγαλύτερη πιθανότητα, να είναι πλέον πολύ υψηλή (να τείνει στο 1) [8].

3.8 Κβαντικές Πύλες 1 qubit και μήτρες του Pauli

Οι κβαντικές πύλες είναι η αντιστοιχία τον κλασσικών λογικών πυλών, οι οποίες χρησιμοποιούνται στους κλασσικούς υπολογιστές για τα κλασσικά bit, στους κβαντικούς υπολογιστές και τα κβαντικά bit [8].

Αυτό που τις διαχωρίζει σημαντικά από τις κλασσικές πύλες, είναι ότι όλες είναι αντιστρέψιμες, σε αντίθεση με κάποιες κλασσικές πύλες, όπως η πύλη NAND. Αυτό σημαίνει ότι πάντα πρέπει να είναι εφικτό, σε ένα κβαντικό σύστημα, να επιστρέψουμε στην αρχική κατάσταση. Ένα κβαντικό σύστημα δεν χάνει ποτέ πληροφορία με το πέρασμα του χρόνου [8].

Οι κβαντικές πύλες εφαρμόζονται στην αρχική μας κβαντική κατάσταση διαδοχικά και αλλάζουν την κατάσταση του συστήματος. Κάθε πύλη πρέπει να αντιστοιχεί σε έναν Unitary πίνακα $(δηλαδή\ έναν\ πίνακα\ U\ για\ τον\ οποίο\ ισχύει: U^tU = 1)$. Στην ουσία, αντιστοιχούν στους γραμμικούς τελεστές, τους οποίους είδαμε παραπάνω (2.2), και εκτελούν κβαντικούς μετασχηματισμούς. Επίσης, αξίζει να σημειώσουμε ότι κάθε κβαντική πύλη, δηλαδή κάθε μοναδιαίος κβαντικός μετασχηματισμός, μετατρέπει το διάνυσμα βάσης του χώρου Hilbert [8].

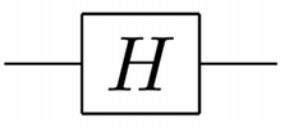
Κάποιες πολύ βασικές κβαντικές πύλες, οι οποίες χρησιμοποιούνται κατά τη διάρκεια κβαντικών υπολογισμών είναι οι εξής [8]:

- HADAMARD: H = $\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\ 1 & -1\end{bmatrix}$

  Ματρέπει τις 2 βασικές καταστάσεις ως εξής:

$$H|0\rangle \rightarrow \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

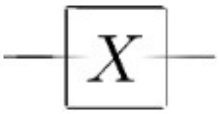
$$H|1\rangle \rightarrow \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$



Εικόνα 3.7: Η πύλη Hadamard [8].

- Pauli – X gate (NOT – bit flip): X = $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

$$X|0\rangle \rightarrow |1\rangle$$
$$X|1\rangle \rightarrow |0\rangle$$



Εικόνα 3.8: Η πύλη X [8].

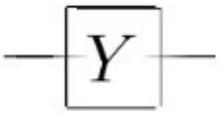
- Pauli – Z gate (phase flip): Z = $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

$$Z|0\rangle \rightarrow |0\rangle$$
$$Z|1\rangle \rightarrow -|1\rangle$$

Εικόνα 3.9: Η πύλη Z [8].

- Pauli – Y gate: Y = -iZX = $\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$

$$Y|0\rangle \rightarrow i|1\rangle$$
$$Y|1\rangle \rightarrow i|0\rangle$$



Εικόνα 3.10: Η πύλη Y [8].

Οι μήτρες του Pauli έχουν όλες την εξής ιδιότητα:

$$X^2 = Y^2 = Z^2 = -iXYZ = I$$

- Phase Shift – R_φ gates: $R_\varphi = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\varphi} \end{bmatrix}$

  Αποτελεί μια οικογένεια από πύλες 1-qubit, οι οποίες αφήνουν την βασική κατάσταση $|0\rangle$ απαράλλαχτη και αντιστοιχίζουν την βασική κατάσταση $|1\rangle$ στην $e^{i\varphi}|0\rangle$.

  Συχνές γωνίες που χρησιμοποιούνται είναι οι:

$$\varphi = \frac{\pi}{4} \rightarrow T - gate,$$

$$\varphi = \frac{\pi}{2} \rightarrow S - gate,$$

$$\varphi = \pi \rightarrow Z - gate \quad [8]$$

3.9 Κβαντικές Πύλες 2 qubit

3.9.1 Ελεγχόμενες Πύλες (Controlled Gates)

Η πιο γνωστή πύλη δύο qubit είναι η C-NOT πύλη:

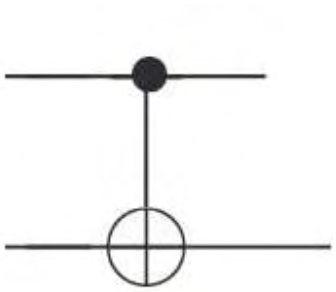
- CNOT (C-NOT): cX = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

  Εκτελεί την εξής μετατροπή:

$$|a, b\rangle \rightarrow |a, a \oplus b\rangle$$

  Δηλαδή, όταν το controlled qubit = $|1\rangle$, αντιστρέφεται το target qubit, αλλιώς δεν κάνει τίποτα.

  Η CNOT χρησιμοποιείται πολύ συχνά για την δημιουργία entangled states.



Εικόνα 3.11: Η πύλη CNOT [8].

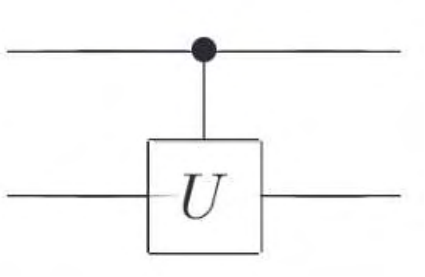
Οι πύλη CNOT μαζί με τις πύλες 1-qubit είναι τα πρωτότυπα για όλες τις κβαντικές πύλες καθώς αποδεικνύεται ότι οποιαδήποτε κβαντική πύλη πολλαπλών qubit μπορεί να φτιαχτεί από τον συνδυασμό CNOT και 1-qubit κβαντικών πυλών. Ένα καθολικό σύνολο κβαντικών πυλών (universal set of quantum gates) αποτελείται από CNOT, H, X, Z και π/8 περιστροφής πύλες [8].

Η πύλη CNOT ανήκει στην γενικότερη κατηγορία των ελεγχόμενων τελεστών/πυλών (Controlled Operations/Gates). Έτσι για ένα γενικό τελεστή U, η πύλη Controlled-U έχει ως εξής:

- C-U: C(U) = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & u_{00} & u_{01} \\ 0 & 0 & u_{10} & u_{11} \end{bmatrix}$

Εκτελεί την εξής μετατροπή:

$$|00\rangle \rightarrow |00\rangle$$
$$|01\rangle \rightarrow |01\rangle$$
$$|10\rangle \rightarrow |1\rangle \otimes U|0\rangle = |1\rangle \otimes (u_{00}|0\rangle + u_{01}|1\rangle)$$
$$|11\rangle \rightarrow |1\rangle \otimes U|1\rangle = |1\rangle \otimes (u_{01}|0\rangle + u_{11}|1\rangle)$$



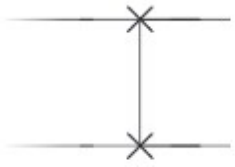
Εικόνα 3.12: Η πύλη controlled-U [8].

3.9.2 Πύλη Αλλαγής (Swap Gate)

- SWAP = $\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

Εκτελεί την εξής μετατροπή:

$$|a, b\rangle \rightarrow |b, a\rangle \quad [8]$$



Εικόνα 3.13: Η πύλη SWAP [8].

3.10 Κβαντικές Πύλες σε 3 qubits

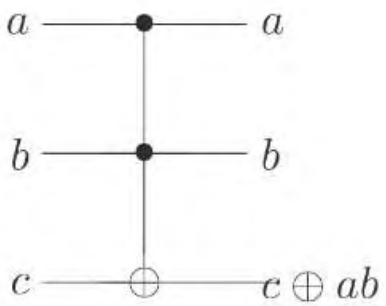
3.10.1 Πύλη Toffoli (CCNOT)

- Toffoli: CCNOT = $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$ [8]

Ο μετατροπές που πραγματοποιεί, μαζί και με την κυκλωματική αναπαράστασή της, φαίνονται στην παρακάτω εικόνα :

Πίνακας 3.2: Αριστερά: Ο πίνακας αληθείας της CCNOT.

Inputs			Outputs		
a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0



Εικόνα 3.14: Δεξιά: Η κυκλωματική αναπαράσταση της CCNOT [8].

3.10.2 Πύλη Fredkin (Controlled Swap)

- Fredkin: CSWAP = $\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$ [9]

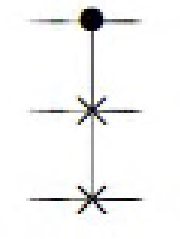
Στην παρακάτω εικόνα φαίνεται η δράση της πύλης Fredkin στα qubit εισόδου:

Πίνακας 3.3: Δράση της πύλης Fredkin στα qubit εισόδου.

$\lvert c_i\, t_{2i}\, t_{1i} \rangle$	$\lvert c_o\, t_{2o}\, t_{1o} \rangle$
$\lvert 000 \rangle$	$\lvert 000 \rangle$
$\lvert 001 \rangle$	$\lvert 001 \rangle$
$\lvert 010 \rangle$	$\lvert 010 \rangle$
$\lvert 011 \rangle$	$\lvert 011 \rangle$
$\lvert 100 \rangle$	$\lvert 100 \rangle$
$\lvert 101 \rangle$	$\lvert 110 \rangle$
$\lvert 110 \rangle$	$\lvert 101 \rangle$
$\lvert 111 \rangle$	$\lvert 111 \rangle$

[9]

Η κυκλωματική της αναπαράσταση φαίνεται παρακάτω:



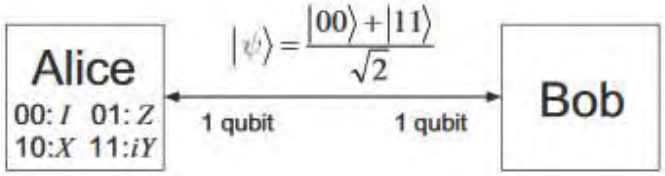
Εικόνα 3.15: Η πύλη Fredkin [8].

ΚΕΦΑΛΑΙΟ 4

Κβαντικά κυκλώματα και εφαρμογές

4.1 Superdense Coding

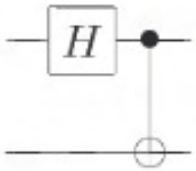
Superdense coding λέγεται ο κβαντικός αλγόριθμος ο οποίος μας επιτρέπει να στείλουμε 2 bit πληροφορίας με 1 qubit, υπό την προϋπόθεση ότι ο δέκτης και ο πομπός εξαρχής μοιράζονται 2 qubit σε μια κατάσταση διεμπλοκής [8].



Εικόνα 4.1: Το κύκλωμα για Superdense Coding [8].

Έστω ότι η Αλίκη έχει ένα μήνυμα που θέλει να μεταφέρει στον Μπομπ, το οποίο αποτελείται από 2 bits (00 ή 01 ή 10 ή 11).

- Προετοιμάζουμε την διαπλεγμένη κατάσταση Bell $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ από τα 2 αρχικά qubits $|0\rangle, |0\rangle$ με την διαδοχική εφαρμογή των κβαντικών πυλών Hadamard και CNOT:



Εικόνα 4.2: Προετοιμασία κατάστασης Bell [8].

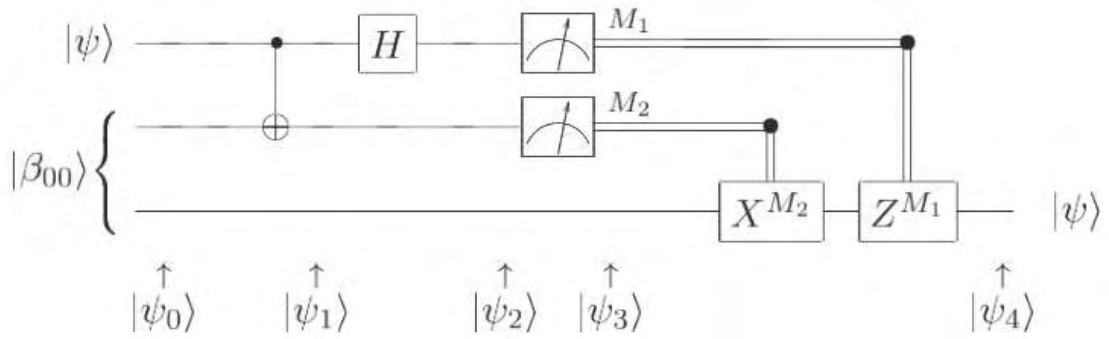
- Στην συνέχεια στέλνουμε στην Αλίκη και τον Μπομπ, οι οποίοι μπορεί να βρίσκονται σε μεγάλη απόσταση, από 1 εκ των 2 διαπλεγμένων qubit.
- Η Αλίκη, ανάλογα του μηνύματος που έχει και θέλει να μεταφέρει στον Μπομπ, εφαρμόζει στο qubit της μια κβαντική πύλη εκ των I, X, Z, XZ (ή iY). Πλέον, η αρχική διαπλεγμένη κατάσταση έχει μετατραπεί σε μία εκ των τεσσάρων καταστάσεων Bell.
  - Κλασσικό μήνυμα: $00 \rightarrow$ Εφαρμογή I: $|\psi\rangle = B_{00} = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$,
  - Κλασσικό μήνυμα: $01 \rightarrow$ Εφαρμογή X: $|\psi\rangle = B_{01} = \frac{|01\rangle+|10\rangle}{\sqrt{2}}$,
  - Κλασσικό μήνυμα: $10 \rightarrow$ Εφαρμογή Z: $|\psi\rangle = B_{10} = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$,
  - Κλασσικό μήνυμα: $11 \rightarrow$ Εφαρμογή $iY = ZX$: $|\psi\rangle = B_{11} = \frac{|01\rangle-|10\rangle}{\sqrt{2}}$
- Τώρα η Αλίκη στέλνει το qubit της στον Bob μέσω ενός κβαντικού δικτύου, ο οποίος εφαρμόζει στην σειρά μια πύλη CNOT (με control qubit αυτό που του έστειλε η Αλίκη) και αμέσως μετά μια Hadamard πύλη στο 1ο qubit που πλέον διαθέτει. Έτσι η κατάσταση του συστήματος που διαθέτει πλέον γίνεται:
  - $B_{00} \rightarrow |00\rangle$
  - $B_{01} \rightarrow |01\rangle$

- $B_{10} \rightarrow |10\rangle$
- $B_{11} \rightarrow |11\rangle$

- Τέλος, ο Bob κάνει μέτρηση της κβαντικής του κατάστασης. Από το αποτέλεσμα που θα πάρει μπορεί να συμπεράνει το 2-bit μήνυμα που ήθελε να του μεταφέρει η Αλίκη:
  - $|00\rangle \rightarrow \eta\ Αλίκη\ του\ έστειλε\ το\ 00$
  - $|01\rangle \rightarrow \eta\ Αλίκη\ του\ έστειλε\ το\ 10$
  - $|10\rangle \rightarrow \eta\ Αλίκη\ του\ έστειλε\ το\ 01$
  - $|11\rangle \rightarrow \eta\ Αλίκη\ του\ έστειλε\ το\ 11$ [8].

4.2 Κβαντική Τηλεμεταφορά (Quantum Teleportation)

Κβαντική τηλεμεταφορά είναι ένας κβαντικός αλγόριθμος που μεταφέρει μια κβαντική κατάσταση από απόσταση [8].



Εικόνα 4.3: Κύκλωμα κβαντικής τηλεμεταφοράς [8].

- Η Αλίκη βρίσκεται σε πολύ μεγάλη απόσταση από τον Μπομπ και αρχικά έχει ένα qubit στην κατάσταση:
$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle.$$
- Ένα τρίτο πρόσωπο προετοιμάζει 2 διαπλεγμένα qubits σε μια οποιαδήποτε κατάσταση Bell, π.χ. την $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$, και στέλνει από 1 qubit στην Αλίκη και τον Μπομπ. Η κατάσταση την οποία προετοιμάζει είναι συμφωνημένη εκ των προτέρων.
- Πλέον η Αλίκη έχει 2 qubits στην κατοχή της, αυτό που θέλει να τηλεμεταφέρει, και το ένα από το ζεύγος διεμπλοκής.
  Η κοινή κατάσταση των 3 qubit πλέον είναι:
$$|\psi_0\rangle = (\alpha|0\rangle + \beta|1\rangle)\frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}$$
- Τώρα η Αλίκη πραγματοποιεί μια μέτρηση κατάστασης στην βάση Bell στα qubit της, η οποία γίνεται με διαδοχική εφαρμογή μιας CNOT και μιας Hadamard πύλης και έπειτα μέτρηση. Το αποτέλεσμα αυτής της διαδικασίας γίνεται ιδιαίτερα εμφανές αν εκφράσουμε την κατάσταση $|\psi_0\rangle$ ως προς τη βάση Bell.
  Οι καταστάσεις Bell :
$$|B_0\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|B_1\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$
$$|B_2\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$
$$|B_3\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Άρα:

$$|00\rangle = \frac{|B_0\rangle + |B_2\rangle}{\sqrt{2}}$$
$$|01\rangle = \frac{|B_1\rangle + |B_3\rangle}{\sqrt{2}}$$
$$|10\rangle = \frac{|B_1\rangle - |B_3\rangle}{\sqrt{2}}$$
$$|11\rangle = \frac{|B_0\rangle - |B_2\rangle}{\sqrt{2}}$$

Τώρα μπορούμε να εκφράσουμε την κοινή κατάσταση των 3 qubit ως εξής:

$$|\psi_0\rangle = \frac{\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle}{\sqrt{2}}$$
$$= \frac{|B_0\rangle(\alpha|0\rangle + \beta|1\rangle) + |B_1\rangle(\alpha|1\rangle + \beta|0\rangle) + |B_2\rangle(\alpha|0\rangle - \beta|1\rangle) + |B_3\rangle(\alpha|1\rangle - \beta|0\rangle)}{2}$$

Η πιθανότητα όλων των πιθανών αποτελεσμάτων της μέτρησης ($|B_0\rangle, |B_1\rangle, |B_2\rangle, |B_3\rangle$) είναι:

$$Prob(B_0) = Prob(B_1) = Prob(B_2) = Prob(B_3) = \left(\frac{1}{2}\right)^2 = \frac{1}{4}$$

Τα 4 πιθανά a posterior states ανάλογα με το αποτέλεσμα μέτρησης της Αλίκης είναι:

- $00 \rightarrow |\psi_3(00)\rangle = \alpha|0\rangle + \beta|1\rangle = |B_0\rangle = I|\psi\rangle$
- $01 \rightarrow |\psi_3(01)\rangle = \alpha|1\rangle + \beta|0\rangle = X|\psi\rangle$
- $10 \rightarrow |\psi_3(10)\rangle = \alpha|0\rangle - \beta|1\rangle = Z|\psi\rangle$
- $11 \rightarrow |\psi_3(11)\rangle = \alpha|1\rangle - \beta|0\rangle = ZX|\psi\rangle$,
  $όπου\ ZX\ σημαίνει\ εφαρμογή\ πρώτα\ της\ πύλης\ X\ και\ μετά\ της\ Z$

(Στην ουσία η πληροφορία που παίρνουμε από αυτό το βήμα είναι «ποια λειτουργία απαιτείται για να ανακτήσουμε το $|\psi\rangle$».)

- Τώρα η Αλίκη στέλνει την κλασσική πληροφορία του αποτελέσματός της μέσω κάποιου φυσικού μέσου τηλεπικοινωνίας στον Μπομπ.
  (Αυτό το βήμα απαγορεύει στην ουσία την επικοινωνία με ταχύτητα μεγαλύτερη της ταχύτητας του φωτός.)
- Ο Μπομπ, δεδομένων των αποτελεσμάτων της μέτρησης της Αλίκης και γνωρίζοντας πλέον την a posterior state, εκτελεί μία εκ των 4 αντίστοιχων αντίστροφων ενεργειών ($I^{-1}, \mathrm{X}^{-1}, \mathrm{Z}^{-1}, (\mathrm{XZ})^{-1}$) στο δικό του μισό του διαπλεγμένου ζεύγους:
  - $00 \rightarrow I$
  - $01 \rightarrow X$
  - $10 \rightarrow Z$
  - $11 \rightarrow ZX$

- Ο Μπομπ έχει πλέον ανακτήσει την αρχική κβαντική κατάσταση της Αλίκης:

$$|\psi_4\rangle = |\psi\rangle \text{ [8]}$$

4.3 Κβαντικός Μετασχηματισμός Fourier (QFT)

Ο κβαντικός μετασχηματισμός Fourier είναι ένας μοναδιαίος τελεστής στον μιδαγικό χώρο Hilbert, τον οποίο χρησιμοποιούμε για να μετρήσουμε οποιοδήποτε ket στο πεδίο της συχνότητας. Είναι κρίσιμο κομμάτι κάποιων κβαντικών αλγορίθμων [5].
Ας υπενθυμίσουμε, αρχικά, τι είναι ο διακριτός μετασχηματισμός Fourier (DFT). Είναι το αντίστοιχο του συνεχή μετασχηματισμού Fourier, αλλά στον πεπερασμένο, διακριτό χρόνο. Αποτελεί την αναπαράσταση σημάτων πεπερασμένου, διακριτού χρόνου, στο πεδίο της συχνότητας.

$X[k] = \sum_{n=0}^{N-1} x[n] e^{-\frac{i2\pi nk}{N}} = \sum_{n=0}^{N-1} x[n] \left[\cos\left(\frac{2\pi kn}{n}\right) - i \cdot sin\left(\frac{2\pi kn}{N}\right)\right]$ *, όπου η τελευταία έκφραση προκύπτει από τον τύπο του Euler (*$e^{ix} = cosx + i \cdot sinx$*).*

Όπου:

- k η συχνότητα στην οποία υπολογίζουμε τον DFT $(\mathrm{k} = 0, 1, \dots, \mathrm{N} - 1)$
- $\mathrm{n} = 0, \dots, \mathrm{N} - 1$ τα χρονικά σημεία πάνω στα οποία δειγματοληπτούμε το σήμα εισόδου μας [5]

Ο DFT μπορεί να εκφραστεί και ως πίνακας μετασχηματισμού, ο οποίος εφαρμόζεται σε ένα σήμα με πολλαπλασιασμό.

$$X = Wx$$

Όπου:

- x είναι το σήμα εισόδου
- W είναι ο NxN τετραγωνικός DFT πίνακας
- X είναι το σήμα εξόδου μας, μετά την εφαρμογή του DFT

Με:

$$W = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega & \omega^2 & \cdots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \cdots & \omega^{2(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \cdots & \omega^{(N-1)(N-1)} \end{bmatrix}$$

Όπου:

- $\omega = e^{-\frac{2\pi i}{N}}$
- $\frac{1}{\sqrt{N}}$ είναι ο παράγοντας κανονικοποίησης, ο οποίος είναι εξαιρετικά χρήσιμος, καθώς κάνει δίνει στον DFT πίνακα μας την ιδιότητα του να είναι μοναδιαίος, η οποία είναι απαραίτητη προϋπόθεση για όλες τις κβαντικές πύλες [5]

Έχοντας πει όλα αυτά πλέον ορίζουμε τον DFT να αντιστοιχεί ένα διάνυσμα $x = \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{N-1} \end{bmatrix} \in \mathbb{C}$ σε ένα διάνυσμα $y = \begin{bmatrix} y_0 \\ y_1 \\ \vdots \\ y_{N-1} \end{bmatrix} \in \mathbb{C}$ έτσι ώστε:

$$y_k \equiv \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} e^{\frac{2\pi i j k}{N}} x_j \text{ [5]}$$

Αντίστοιχα, ο κβαντικός μετασχηματισμός Fourier (QFT) κάνει κάτι παρόμοιο. Ο QFT σε μια ορθοκανονική βάση $|0\rangle, |1\rangle, \ldots |N-1\rangle$, ορίζεται ως ο γραμμικός τελεστής που δρα ως εξής στις βασικές καταστάσεις :

$$QFT|j\rangle \equiv \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{\frac{2\pi i j k}{N}} |k\rangle \text{ [8]}$$

Όπου:

- $|j\rangle$ είναι η αρχική μας βασική κατάσταση
- N είναι το μήκος του διανύσματος βάσης
- $|k\rangle$ είναι η συντεταγμένη του νέου διανύσματος βάσης που προκύπτει

- $\frac{1}{\sqrt{\mathrm{N}}}\sum_{\mathrm{k}=0}^{\mathrm{N}-1} \mathrm{e}^{\frac{2\pi \mathrm{ijk}}{\mathrm{N}}}$ είναι τα πλάτη του νέου διανύσματος βάσης

Ισοδύναμα, με λίγες πράξεις, ο QFT μπορεί να εκφραστεί ως ο εξής μετασχηματισμός:

$$|j\rangle \rightarrow \frac{(|0\rangle + e^{(2\pi i[0.j_n])}|1\rangle)(|0\rangle + e^{(2\pi i[0.j_{n-1}\, j_n])}|1\rangle) \cdots (|0\rangle + e^{(2\pi i[0.j_1 j_2 \cdots j_n])}|1\rangle)}{2^{\frac{n}{2}}}$$

Όπου:

- $[0.j_1 j_2 \cdots j_m] = \sum_{k=1}^{m} j_k 2^{-k}$ [5,8]

Η δράση του QFT σε μια τυχαία κατάσταση μπορεί να περιγραφεί ως εξής:

$$\sum_{j=0}^{N-1} x_j |j\rangle \rightarrow \sum_{k=0}^{N-1} y_k |k\rangle$$

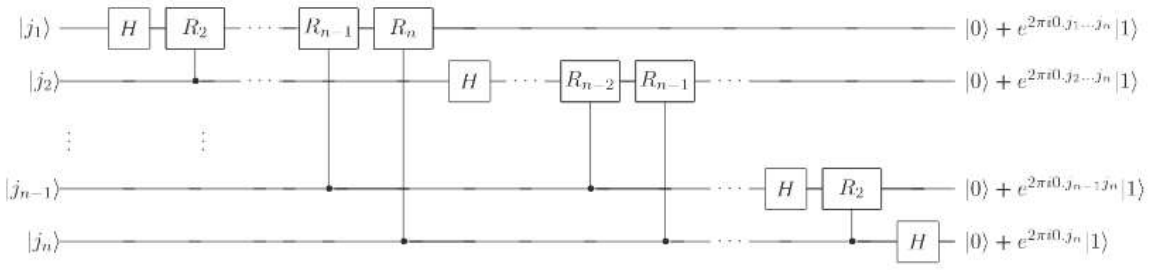
Όπου:

- y_k *είναι ο DFT των πλατών* x_j [5,8]

Ο QFT είναι μοναδιαίος μετασχηματισμός [5,8].

4.3.1 Υλοποίηση του Κβαντικού Μετασχηματισμού Fourier ως Πύλη σε ένα Κβαντικό Κύκλωμα

Το κύκλωμα για την εφαρμογή του QFT φαίνεται παρακάτω:

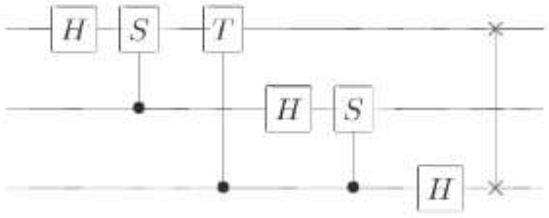


Εικόνα 4.4: Κυκλωματική αναπαράσταση QFT.

Στο τέλος του κυκλώματος μπορούν να προστεθούν SWAP πύλες, για να αντιστραφεί η σειρά των qubit εξόδου.

Η πύλη R_k δηλώνει τον μετασχηματισμό $R_k = \begin{bmatrix} 1 & 0 \\ 0 & e^{\frac{2\pi i}{2^k}} \end{bmatrix}$ [8].

Για παράδειγμα ο QFT για 3 qubits μοιάζει ως εξής:



Εικόνα 4.5: Κυκλωματική αναπαράσταση QFT για 3 qubits [8].

Υπενθύμιση: S είναι η phase πύλη και T η π/8 πύλη.

Και σε μορφή πίνακα:

$$QFT_{2^3} = \frac{1}{\sqrt{2^3}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 & \omega^5 & \omega^6 & \omega^7 \\ 1 & \omega^2 & \omega^4 & \omega^6 & 1 & \omega^2 & \omega^4 & \omega^6 \\ 1 & \omega^3 & \omega^6 & \omega^1 & \omega^4 & \omega^7 & \omega^2 & \omega^5 \\ 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 & 1 & \omega^4 \\ 1 & \omega^5 & \omega^2 & \omega^7 & \omega^4 & \omega^1 & \omega^6 & \omega^3 \\ 1 & \omega^6 & \omega^4 & \omega^2 & 1 & \omega^6 & \omega^4 & \omega^2 \\ 1 & \omega^7 & \omega^6 & \omega^5 & \omega^4 & \omega^3 & \omega^2 & \omega^1 \end{bmatrix}$$

Όπου:

$$\omega = e^{\frac{2\pi i}{8}} = \sqrt{i} \quad [8]$$

4.3.2 Εκτίμηση Φάσης (Phase Estimation)

Ο QFT είναι πολύ σημαντικός για την διαδικασία της εκτίμησης φάσης, η οποία είναι σημαντικό κομμάτι πολλών κβαντικών αλγορίθμων.

Σκοπός του αλγορίθμου εκτίμησης φάσης δοσμένου ενός τελεστή U με ιδιοδιανύσματα $|u\rangle$ και ιδιοτιμές $e^{2\pi i\varphi}$, δηλαδή ισχύει: $U|\psi\rangle = e^{2\pi i\varphi}|\psi\rangle$, όπου το φ είναι άγνωστο, είναι ο υπολογισμός του φ. Ο αλγόριθμος εκτίμησης φάσης είναι εργαλείο, μια διαδικασία, η οποία χρησιμοποιείται ενσωματωμένη σε άλλους αλγορίθμους για την εκτέλεση ενδιαφέροντων υπολογιστικών έργων [8].

Ο αλγόριθμος έχει ως εξής:

Ο πρώτος καταχωρητής έχει t qubits στην κατάσταση $|0\rangle$, όπου το t εξαρτάται από την ακρίβεια εκτίμησης του φ που επιθυμούμε και την πιθανότητα ορθής εκτίμησης φάσης που επιθυμούμε να έχουμε. Ο δεύτερος καταχωρητής ξεκινάει στην κατάσταση $|u\rangle$ και περιέχει όσα qubits χρειάζονται για να αποθηκευτεί η $|u\rangle$.

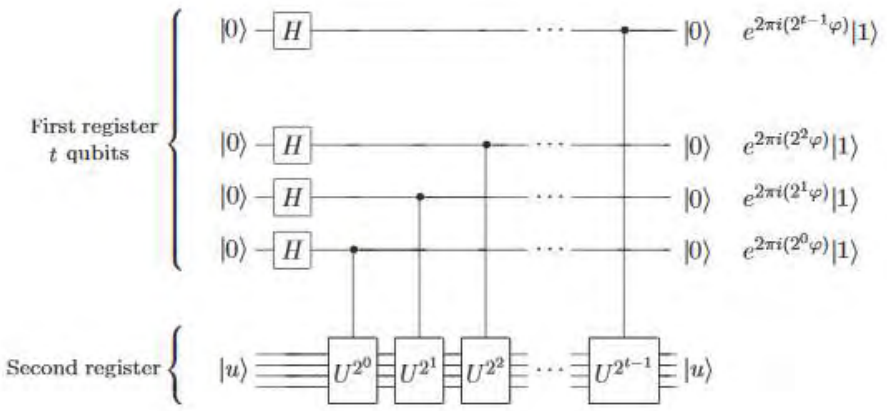
Ο αλγόριθμος αποτελείται από 3 κομμάτια:

1. Εφαρμόζουμε μια Hadamard Πύλη στον πρώτο καταχωρητή και αμέσως μετά μια Controlled-U πράξη ανάμεσα στον πρώτο και τον δεύτερο καταχωρητή, όπου το U είναι υψωμένο σε διαδοχικές δυνάμεις του 2. Η τελική κατάσταση του πρώτου καταχωρητή που προκύπτει είναι η:

$$\frac{1}{2^{\frac{t}{2}}}\left(|0\rangle + e^{2\pi i 2^{t-1}\varphi}|1\rangle\right)\left(|0\rangle + e^{2\pi i 2^{t-2}\varphi}|1\rangle\right)\cdots\left(|0\rangle + e^{2\pi i 2^{0}\varphi}|1\rangle\right)$$

$$= \frac{1}{2^{\frac{t}{2}}}\sum_{k=0}^{2^t-1} e^{2\pi i\varphi k}\,|k\rangle$$

Η τελική κατάσταση του δεύτερου καταχωρητή παραμένει η $|u\rangle$.



Εικόνα 4.6: Πρώτα βήμα του αλγορίθμου εκτίμησης φάσης [8].

2. Έπειτα, στο δεύτερο στάδιο, εφαρμόζουμε τον Αντίστροφο Κβαντικό Μετασχηματισμό Fourier (Inverse-QFT) στον πρώτο καταχωρητή, το οποίο συμβαίνει αντιστρέφοντας το κύκλωμα του απλού QFT.

Ο αντίστροφος QFT πραγματοποιεί τον εξής μετασχηματισμό:

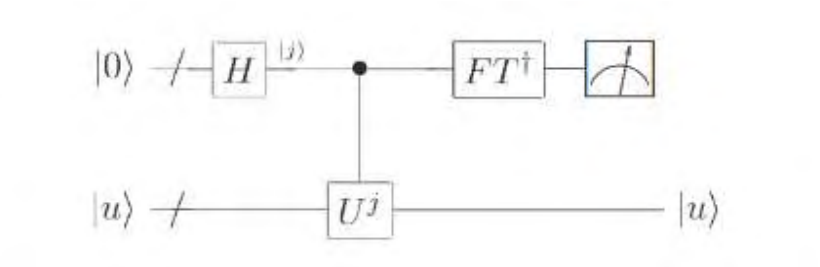
$$\frac{1}{2^{\frac{t}{2}}}\sum_{j=0}^{2^t-1} e^{2\pi i\varphi j}\,|j\rangle|u\rangle \rightarrow |\tilde{\varphi}\rangle|u\rangle$$

Όπου:

- $|\tilde{\varphi}\rangle$ αποτελεί μια κατάσταση η οποία δίνει μια καλή εκτίμηση για το φ, όταν μετρηθεί.

3. Στο τελικό στάδιο διαβάζουμε την κατάσταση του πρώτου qubit εφαρμόζοντας μια μέτρηση στην υπολογιστική βάση.

Ολόκληρος ο αλγόριθμος εκτίμησης φάσης ως κύκλωμα έχει την εξής μορφή:



Εικόνα 4.7: Κυκλωματική αναπαράσταση της διαδικασίας εκτίμησης φάσης [8].

Όπου:

- / δηλώνει μια πλοιάδα κβαντικών καλωδίων
- $|u\rangle$ είναι μια ιδιοκατάσταση του τελεστή U με ιδιοτιμή $e^{2\pi i\varphi}$
- Η κατάσταση εξόδου της μέτρησης είναι μια εκτίμηση του φ με ακρίβεια $t - \left\lceil \log\left(2 + \frac{1}{2e}\right)\right\rceil$ bits και πιθανότητα να είναι επιτυχημένη $1 - \varepsilon$ [8].

4.4 Βασικά στάδια κβαντικού υπολογισμού και η έννοια του κβαντικού παραλληλισμού

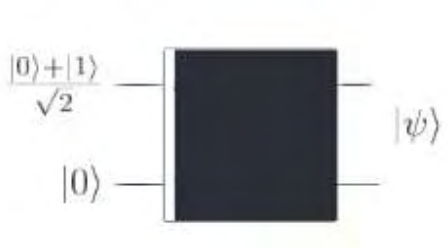
Μπορούμε να προσομοιώσουμε ένα οποιοδήποτε κλασσικό κύκλωμα με κάποιο αντίστοιχο κβαντικό, με την χρήση κβαντικών πυλών Toffoli , οι οποίες χρησιμοποιούνται για να αντικαταστίσουν τις μη-αντιστρέψιμες κλασσικές πύλες, όπως την NAND [8].

Ο κβαντικός παραλληλισμός είναι μια ιδιότητα πολλών κβαντικών αλγορίθμων, η οποία επιτρέπει στους κβαντικούς υπολογιστές να υπολογίζουν μια συνάρτηση f(x) για πολλές διαφορετικές τιμές του x ταυτόχρονα [8].

Παράδειγμα με 2 qubits:

Έστω η συνάρτηση $f(x)$: $\{0,1\} \rightarrow \{0,1\}$ με 1 bit πεδίο ορισμού (domain) και σύνολο τιμών (range). Ο κβαντικός υπολογιστής ξεκινάει τον υπολογισμό με μια κατάσταση $|x, y\rangle$. Με μια αλληλουχία κβαντικών πυλών την οποία απεικονίζουμε ως μαύρο κουτί (black box), μετασχηματίζουμε αυτήν την κβαντική κατάσταση στην κατάσταση $|x, y \oplus f(x)\rangle$, όπου $\oplus$ είναι η λογική πράξη xor (ή ισυδύναμα μια πρόσθεση modulo 2), με το πρώτο qubit να είναι ο καταχωρητής δεδομένων (data) και το δεύτερο ο καταχωρητής στόχος (target). Ο τελεστής που ορίζει τον μετασχηματισμό $|x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$ λέγεται U_f και είναι μοναδιαίος. Αν $y = 0$, τότε η τελευταία τιμή του δεύτερου qubit είναι η τιμή $f(x)$ [8].

Αν τώρα το κύκλωμά μας είχε ως εξής:

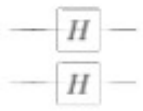


Εικόνα 4.8: Κύκλωμα με μαύρο κουτί (black box) [8].

Τότε η έξοδος του κυκλώματός μας είναι η κατάσταση $\frac{|0,f(0)\rangle+|1,f(1)\rangle}{\sqrt{2}}$. Παρατηρούμε ότι με έναν μόνο μετασχηματισμό η κατάστασή μας περιέχει ταυτόχρονα πληροφορίες τόσο για το f(0) όσο και για το f(1), εκμεταλλευόμενη την ιδιότητα της υπέρθεσης (superposition), που διαθέτουν τα

κβαντικά συστήματα. Βέβαια δεν μπορούμε άμεσα να τις αξιοποιήσουμε και τις δύο, καθώς με την πράξη της μέτρησης, το σύστημά μας θα καταρρεύσει σε μόνο μία εκ των δύο.

Η κατάσταση $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$ προετοιμάστηκε με την εφαρμογή μια Hadamard πύλης σε μια κατάσταση $|0\rangle$. Η παραπάνω διαδικασία μπορεί να γενικευτεί για n qubits, με την μία και μοναδική Hadamard πύλη να αντικαταστάται απο έναν Hadamard μετασχηματισμό (Hadamard/Walsh–Hadamard Transform), ο οποίος δεν είναι τίποτα άλλο παρά n Hadamard πύλες οι οποίες εφαρμόζονται παράλληλα, και συμβολίζεται ως $H^{\otimes n}$:



Εικόνα 4.9: Walsh-Hadamard μετασχηματισμός με 2 πύλες Hadamard [8].

Το αποτέλεσμα ενός τέτοιου μετασχηματισμού είναι η κατάσταση:

$\frac{1}{\sqrt{2^n}}\sum_x|x\rangle$, όπου x είναι όλες οι πιθανές τιμές της κατάστασής μας. Το αποτέλεσμά αυτό είναι μια υπέρθεση όλων των πιθανών καταστάσεων με ίσα πλάτη πιθανότητας. Πολύ σημαντικά, παρατηρούμε ότι μόλις με n πύλες παράξαμε 2^n καταστάσεις [8].

Στην γενική κατάσταση όπου έχουμε n+1 bit εισόδου και επιδιώκουμε 1 bit εξόδου, ο κβαντικός παράλληλος υπολογισμός έχει ως εξής:

1. Προετοιμάζουμε την n+1 qubit κβαντική κατάσταση $|0\rangle^{\otimes n}|0\rangle$
2. Εφαρμόζουμε μετασχηματισμό Hadamard στα πρώτα n qubit ($H^{\otimes n}$)
3. Εφαρμόζουμε τον μετασχηματισμό U_f και παίρνουμε την κατάσταση:

$$\frac{1}{\sqrt{2^n}}\sum_x|x\rangle|f(x)\rangle$$

Και εδώ, δηλαδή στην περίπτωση των n+1 qubit, η μέτρηση της κατάστασης θα μας δώσει μόνο μία εκ των τιμών της f(x) για κάποιο συγκεκριμένο x. Έτσι, οι πληροφορίες που έχουμε για όλες τις πιθανές καταστάσεις δεν είναι άμεσα διαθέσιμες. Για να γίνει πραγματικά χρήσιμος ο

κβαντικός παραλληλισμός πρέπει να έχουμε την δυνατότητα να εξάγουμε πληροφορίες για περισσότερες από μία τιμές της f(x) από καταστάσεις υπέρθεσης όπως η $\sum_x |x\rangle|f(x)\rangle$ [8].

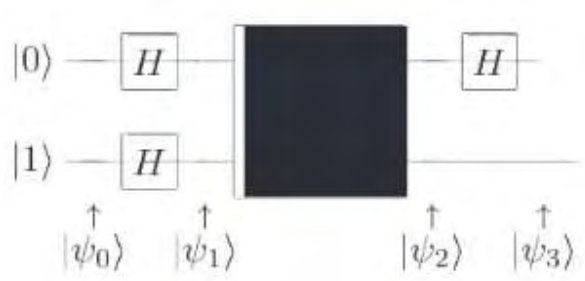
4.5 Οι αλγόριθμοι των Deutsch και Deutsch-Jozsa

4.5.1 Ο αλγόριθμος Deutsch

Ο αλγόριθμος του Deutsch συνδυάζει τον κβαντικό παραλληλισμό με την ιδιότητα της παρεμβολής (Wave Interference), η οποία είναι εγγενής στα κβαντικά συστήματα [8].

Επίσης θα δούμε για πρώτη φορά την έννοια του «Προφήτη» (Oracle), ο οποίος είναι ένα θεωρητικό εργαλείο που χρησιμοποιείται στους κβαντικούς αλγορίθμους. Εκτελεί θεωρητικά μια πολύ συγκεκριμένη λειτουργία-μετασχηματισμό, χωρίς να δίνονται λεπτομέρειες για την κατασκευή του και το πώς το πετυχαίνει αυτό. Συνήθως απεικονίζεται ως ένα μαύρο κουτί [8].

1. Το 1ο qubit προετοιμάζεται μέσω μιας πύλης Hadamard στην κατάσταση $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$. Αυτήν την φορά, το 2ο qubit, αντί να βρίσκεται στην κατάσταση $|0\rangle$, προετοιμάζεται στην κατάσταση $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$, με το πέρασμα μιας κβαντικής κατάστασης $|1\rangle$ από μια Πύλη Hadamard.



Εικόνα 4.10: 1ο βήμα του αλγορίθμου Deutsch [8].

2. Η κατάσταση $|\psi_1\rangle$ τώρα είναι η:

$$\left[\frac{|0\rangle+|1\rangle}{\sqrt{2}}\right]\otimes\left[\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right]=\frac{|00\rangle-|01\rangle+|10\rangle-|11\rangle}{2}$$

3. Εφαρμόζοντας τον μετασχηματισμό U_f (από το κεφάλαιο 4.4) τώρα στην $|\psi_1\rangle$ παίρνουμε μια από τις εξής καταστάσεις:

$$|\psi_2\rangle = \begin{cases} \pm\left[\frac{|0\rangle + |1\rangle}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \alpha\nu\, f(0) = f(1) \\ \pm\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \alpha\nu\, f(0) \neq f(1) \end{cases}$$

4. Η τελευταία πύλη Hadamard στο 1ο qubit τώρα μας δίνει την κατάσταση:

$$|\psi_3\rangle = \begin{cases} \pm|0\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \alpha\nu\, f(0) = f(1) \\ \pm|1\rangle \otimes \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right], \alpha\nu\, f(0) \neq f(1) \end{cases}$$

Αλλά καθώς η συνάρτηση $f(x)$ μπορεί να πάρει μόνο τις τιμές 0,1, παρατηρούμε ότι:

$$f(0) \oplus f(1) = \begin{cases} 0\,, \alpha\nu\, f(0) = f(1) \\ 1\,, \alpha\nu\, f(0) \neq f(1) \end{cases}$$

Και ξαναγράφουμε την $|\psi_3\rangle$ ως:

$$|\psi_3\rangle = \pm|f(0) \oplus f(1)\rangle \left[\tfrac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$ [8].

Παρατηρούμε ότι μόνο με την πράξη μέτρησης του 1ο qubit, προσδιορίζουμε μιας ιδιότητα της $f(x)$, συγκεκριμένα την τιμή του $f(0) \oplus f(1)$. Σε έναν κλασσικό υπολογιστή, ο προσδιορισμός της αντίστοιχης τιμής του XOR, θα απαιτούσε τουλάχιστον 2 υπολογισμούς.

Αυτό που είναι πολύ σημαντικό και παρατηρούμε από τον αλγόριθμο του Deutsch, αλλά και γενικότερα από τους κβαντικούς αλγορίθμους, είναι ότι με μια έξυπνη επιλογή συνάρτησης και τελικού τελεστή, μπορούμε να εξάγουμε πολύ αποδοτικά πληροφορίες για την συνάρτησή μας. Πιο αποδοτικά από έναν κλασσικό υπολογιστή [8].

4.5.2 Ο αλγόριθμος των Deutsch-Jozsa

Ο αλγόριθμος Deutsch-Jozsa αποτελεί την γενίκευση του αλγορίθμου Deutsch. Το πρόβλημα του Deutsch έχει ως εξής:

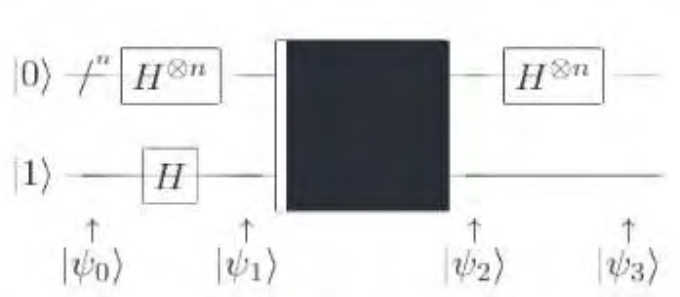
Η Αλίκη, στο Amsterdam, διαλέγει έναν αριθμό x στο εύρος $[0, \cdots, 2^n - 1]$, και τον στέλνει στον Μπομπ, στη Βοστόνη. Ο Μπομπ υπολογίζει το αποτέλεσμα μιας συνάρτησης με είσοδο το x, την f(x), και στέλνει το αποτέλεσμα στην Αλίκη, το οποίο είναι 0 ή 1. Η συνάρτηση του Μπομπ

είναι είτε σταθερή (constant), είτε ισορροπημένη (balanced) (0 για τις μισές τιμές του x και 1 για τις άλλες μισές). Σκοπός της Αλίκης είναι να συμπεράνει με σιγουριά τι είδους συνάρτηση χρησιμοποίησε ο Μπομπ, σταθερή ή ισορροπημένη, επικοινωνώντας μαζί του το λιγότερο δυνατό. Πόσο γρήγορα μπορεί να τα καταφέρει;

Στην κλασσική περίπτωση, εξετάζοντας την χειρότερη περίπτωση, η Αλίκη μπορεί να θέλει να επικοινωνήσει, ρωτώντας τον Μπομπ για την τιμή του x, τουλάχιστον $\frac{2^n}{2} + 1$ φορές, καθώς μπορεί να λάβει στη σειρά $\frac{2^n}{2}$ '0', πριν λάβει έστω και ένα '1', το οποίο θα της έλεγε ότι η συνάρτηση είναι ισορροπημένη και όχι σταθερή. Ο καλύτερος ντετερμινιστικός αλγόριθμος, λοιπόν, ο οποίος μπορεί να χρησιμοποιήσει, χρησιμοποιεί τουλάχιστον $\frac{2^n}{2+1}$ ερωτήματα (queries). Επιπλέον, σε κάθε γράμμα με ερώτημα η Αλίκη στέλνει n bits πληροφορίας. Τέλος, ο υπολογισμός της f(x) μπορεί να είναι εγγενώς δύσκολος, το οποίος θα ανέβαζε το κόστος του, μαζί με την φυσική απόσταση που χωρίζει τον Μπομπ και την Αλίκη [8].

Ωστόσο, αν ο Μπομπ και η Αλίκη αντάλλαζαν qubits αντί για κλασσικά bits πληροφορίας, με την συμφωνία ότι ο Μπομπ θα υπολογίσει την f(x) χρησιμοποιώντας τον μοναδιαίο μετασχηματισμό U_f, τότε η Αλίκη θα μπορούσε να προσδιορίσει την φύση της f(x), με μία μόνο αλληλεπίδραση με τον Μπομπ, με τον ακόλουθο αλγόριθμο:

Η Αλίκη έχει έναν καταχωρητή n qubits, στον οποίο αποθηκεύει τα ερωτήματά της και και έναν καταχωρητή 1 qubit, τον οποίο στέλνει στον Μπομπ για να αποθηκεύει τις απαντήσεις του. Προετοιμάζει και τους 2 καταχωρητές σε κατάσταση υπέρθεσης. Ο Μπομπ με τη σειρά του θα υπολογίσει την τιμή του f(x) χρησιμοποιώντας κβαντικό παραλληλισμό και θα αποθηκεύσει την απάντησή του στον κατάλληλο καταχωρητή. Στην συνέχεια η Αλίκη παρεμβάλει τις καταστάσεις του καταχωρητή ερωτημάτων χρησιμοποιώντας Hadamard μετασχηματισμό και τελειώνει, κάνοντας μια κατάλληλη μέτρηση για να προσδιορίσει εάν η f(x) είναι σταθερή ή ισορροπημένη.



Εικόνα 4.11: Κυκλωματική αναπαράσταση του αλγορίθμου Deutsch-Jozsa [8].

1. Η κατάσταση εισόδου, όπως φαίνεται και από το σχήμα είναι η:

$$|\psi_0\rangle = |0\rangle^{\otimes n} \otimes |1\rangle$$

2. Μετά την εφαρμογή του μετασχηματισμού Hadamard στους 2 καταχωρητές προκύπτει η κατάσταση:

$$|\psi_1\rangle = \sum_{x\in\{0,1\}^n} \frac{|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

Όπου:

- $x \in \{0,1\}^n$ δηλώνει ότι το έχουμε άθροισμα για όλες τις βασικές καταστάσεις n qubits (π.χ. αν n=2: $|00\rangle + |01\rangle + |10\rangle + |11\rangle$)

Δηλαδή ο καταχωρητής ερωτημάτων βρίσκεται σε υπέρθεση όλων των πιθανών καταστάσεων και ο καταχωρητής απάντησης σε ισοπίθανη υπέρθεση των καταστάσεων $|0\rangle$ $και$ $|1\rangle$.

3. Τώρα ο Μπομπ εφαρμόζει τον μετασχηματισμό $U_f : |x, y\rangle \rightarrow |x, y \oplus f(x)\rangle$, δηλαδή υπολογίζει την συνάρτηση f(x).

$$|\psi_2\rangle = \sum_{x\in\{0,1\}^n} \frac{(-1)^{f(x)}|x\rangle}{\sqrt{2^n}} \left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right] = \frac{1}{\sqrt{2^{n+1}}} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}|x\rangle(|0\rangle - |1\rangle)$$

Παρατηρούμε ότι η τιμή της συνάρτησης f(x) κρύβεται ως πλάτος πιθανότητας της κατάστασης υπέρθεσης ενός qubit.

4. Η αλίκη τώρα εφαρμόζει τον μετασχηματισμό Hadamard στον πρώτο καταχωρητή.

   Κάνοντας χρήση του τύπου:

$$H^{\otimes n}|x\rangle = \sum_{z\in\{0,1\}^n} \frac{(-1)^{x\cdot z}|z\rangle}{\sqrt{2^n}}$$

   Όπου:

   - $x \cdot z$ δηλώνει το εσωτερικό γινόμενο τον x, z, mod 2, δηλαδή:

$$x \cdot z = x_0 y_0 \oplus x_1 y_1 \oplus \cdots x_{n-1} y_{n-1}$$

   Προκύπτει ότι η Αλίκη παίρνει την κατάσταση:

$$|\psi_3\rangle = \sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} \frac{(-1)^{x\cdot z + f(x)}|z\rangle}{2^n}\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

$$= \frac{1}{2^n} \sum_{z\in\{0,1\}^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)}(-1)^{x\cdot z}|z\rangle\left[\frac{|0\rangle - |1\rangle}{\sqrt{2}}\right]$$

   Ας παρατηρήσουμε τώρα την κατάσταση $|\psi_3\rangle$, όταν η f(x) είναι σταθερή και αντίστοιχα όταν είναι ισορροπημένη, για την κατάσταση στο 1ο qubit $|z\rangle = |0\rangle^{\otimes n}$. Συγκεκριμένα, ας παρατηρήσουμε το πλάτος πιθανότητας του 1ου qubit:

   - Για $|z\rangle = |0\rangle^{\otimes n}$ και f(x) σταθερή (f(x)=c, όπου $c \in \{0,1\}$), έχουμε:

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^c = \begin{cases} 1, \alpha\nu\ c = 0 \\ -1, \alpha\nu\ c = 1 \end{cases}$$

   - Για $|z\rangle = |0\rangle^{\otimes n}$ και f(x) ισορροπημένη, έχουμε:

$$\frac{1}{2^n} \sum_{x\in\{0,1\}^n} (-1)^{f(x)} = 0$$

5. Η Αλίκη τώρα μετράει τον καταχωρητή ερωτήματος. Εξετάζοντας την πιθανότητα να μετρήσουμε $|0\rangle^{\otimes n}$, προκύπτει:

$$\left|\frac{1}{2^n}\sum_{x=0}(-1)^{f(x)}\right|^2$$

Το οποίο βγαίνει 0 (0% πιθανότητα να μετρήσουμε $|0\rangle^{\otimes n}$) , εάν η f(x) είναι ισορροπημένη και 1 (100% πιθανότητα να μετρήσουμε $|0\rangle^{\otimes n}$), εάν η f(x) είναι σταθερή.

Επομένως, η Αλίκη αν μετρήσει μόνο '0', η f είναι σταθερή, σε διαφορετική περίπτωση η f είναι ισορροπημένη.

Επομένως λύσαμε ένα πρόβλημα που απαιτούσε $\frac{2^n}{2}+1$ υπολογισμούς σε 1 υπολογισμό μόνο. Αυτή, προφανώς, είναι μια εκπληκτική βελτίωση [8].

Ωστόσο, το πρόβλημα του Deutsch δεν έχει κάποια πρακτική εφαρμογή που να μπορούμε να χρησιμοποιήσουμε στην καθημερινότητα μέχρι στιγμής. Επίσης, οι μέθοδοι υπολογισμού μιας κλασσικής συνάρτησης και μιας κβαντικής διαφέρουν τελείως, οπότε η σύγκριση πολυπλοκότητας δεν είναι ακριβώς έγκυρη. Τέλος, σε έναν κλασσικό υπολογιστή, η Αλίκη θα μπορούσε να λύσει το πρόβλημα με λίγες επαναλήψεις, ζητώντας από τον Μπομπ να υπολογίσει την τιμή f(x) για μερικά τυχαία x, πολύ σύντομα με μεγάλη πιθανότητα ακρίβεια.

Ωστόσο, ο αλγόριθμος Deutsch–Jozsa δεν παύει να έχει μεγάλο θεωρητικό ενδιαφέρον και να αποτελεί βάση για πιο περίπλοκους, αλλά και πρακτικούς, κβαντικούς αλγορίθμους [8].

4.6 Ο αλγόριθμος του Grover για αναζήτηση σε μη-δομημένες συλλογές δεδομένων

Ο αλγόριθμος του Grover είναι ένας κβαντικός αλγόριθμος αναζήτησης, ο οποίος επιτυγχάνει την μείωση την πολυπλοκότητας χρόνου αναζήτησης σε μια μη-δομημένη συλλογή δεδομένων, από $O(N)$, που θα έπαιρνε σε έναν κλασσικό υπολογιστή, σε $O\left(\sqrt{N}\right)$. Αν δηλαδή η διαδικασία σε έναν κλασσικό υπολογιστή έπαιρνε 1.000.000 βήματα στην χειρότερη περίπτωση, σε έναν κβαντικό με τη χρήση του αλγορίθμου του Grover θα έπαιρνε 1.000 βήματα [8,12].

Γιατί, όμως, $O(N)$; Αν είχαμε μια λίστα με N στοιχεία και το στοιχείο που ψάχναμε ήταν, τυχαία, στην τελευταία θέση, δεν θα μπορούσαμε παρά να αναζητήσουμε το στοιχείο θέση-θέση μέχρι να φτάσουμε στην τελευ

ταία, όπου και βρίσκεται.

Πώς επιτυγχάνεται αυτό;

Έστω ότι έχουμε μια λίστα με N στοιχεία, με δείκτες από 0 έως N-1, οι οποίοι εκφράζονται στο δυαδικό σύστημα αρίθμησης (π.χ. αν έχουμε 8 στοιχεία, έχουμε 3-bit δείκτες, για να αποθηκευτεί η πληροφορία αρίθμησής τους).
Στην αναζήτηση που θα εκτελέσουμε σε αυτήν την λίστα υπάρχουν ακριβώς M λύσεις, όπου: $1 \leq M \leq N$.
Επιπλέον, έχουμε μια συνάρτηση f, η οποία έχει έξοδο 1, όταν παίρνει ως είσοδο την τιμή που αναζητούμε (π.χ. w) και έξοδο 0, όταν παίρνει ως είσοδο οποιαδήποτε άλλη τιμή (π.χ. x).
Έχουμε ένα 'μαύρο κουτί', το οποίο αποκαλούμε 'Προφήτη' (μια τεχνική που χρησιμοποιείται συχνά στους κβαντικούς αλγορίθμους), του οποίου την ακριβή πολυπλοκότητα δεν γνωρίζουμε, ο οποίος εκτελεί τον εξής μετασχηματισμό:

$$|x\rangle|q\rangle \xrightarrow{O} |x\rangle|q \oplus f(x)\rangle,$$

Όπου:

- x είναι ο καταχωρητής του δείκτη της λίστας
- $|q\rangle$ είναι ένα qubit το οποίο αντιστρέφεται αν $f(x) = 1$, ειδάλλως παραμένει σταθερό.

Μπορούμε να ελέγξουμε αν το x είναι η λύση μας, προετοιμάζοντας την κατάσταση $|x\rangle|0\rangle$, εφαρμόζοντας τον προφήτη, και τέλος ελέγχοντας αν το qubit $|q\rangle$ αντιστράφηκε σε $|1\rangle$ ή όχι.

Το qubit $|q\rangle$ το προετοιμάζουμε στην κατάσταση $\frac{|0\rangle-|1\rangle}{\sqrt{2}}$. Τότε, η λειτουργία του προφήτη είναι η εξής:

$$|x\rangle\left(\frac{|0\rangle-|1\rangle}{\sqrt{2}}\right)\overset{O}{\rightarrow}(-1)^{f(x)}|x\rangle(\frac{|0\rangle-|1\rangle}{\sqrt{2}})$$

Ή πιο απλά, αφού η τιμή του qubit $|q\rangle$ δεν αλλάζει:

$$|x\rangle\overset{O}{\rightarrow}(-1)^{f(x)}|x\rangle$$

Θα ονομάσουμε αυτόν τον μετασχηματισμό U_f.

Για ένα πρόβλημα με M λύσεις, χρειάζεται να εφαρμόσουμε τον προφήτη $O\left(\sqrt{\frac{N}{M}}\right)$ φορές [8,12].

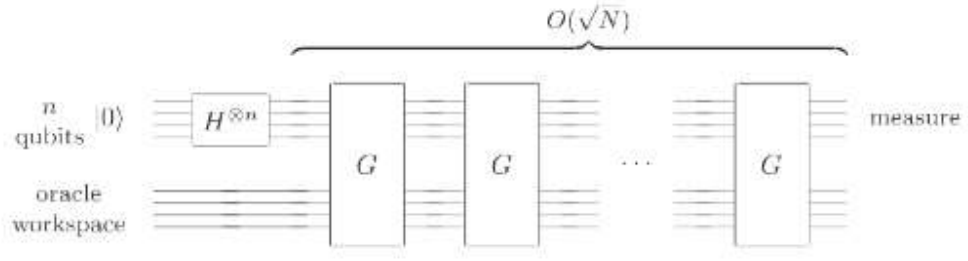
Μέχρι στιγμής έχουμε μιλήσει για ένα 'μαύρο κουτί' ή 'Προφήτη', το οποίο 'δια μαγείας' φαίνεται να ξέρει ακριβώς ποια είναι η λύση στο πρόβλημά μας. Φυσικά αυτό δεν συμβαίνει.

Ο αλγόριθμος, πιο αναλυτικά, χωρίζεται σε 5 βήματα:

0. Προετοιμάζουμε την κατάσταση $|\psi\rangle$, εφαρμόζοντας στα n qubits εισόδου τον μετασχηματισμό Hadamard.

$$|\psi\rangle=\frac{1}{N^{\frac{1}{2}}}\sum_{x=0}^{N-1}|x\rangle$$

Αυτή είναι η ισοπίθανη κατάσταση υπέρθεσης όλων των πιθανών κβαντικών καταστάσεων του $|x\rangle$.



Εικόνα 4.12: Κυκλωματική αναπαράσταση του αλγορίθμου του Grover [8].

Στην συνέχεια ο αλγόριθμος αποτελείται από μια επαναλαμβανόμενη διαδικασία η οποία αποκαλείται «Επανάληψη του Grover» ('G'). Αυτή έχει ως εξής:

1. Εφαρμόζουμε, κάπως, τον μετασχημασχηματισμό U_f (εδώ πάλι αναπόφευκτα εισάγουμε την έννοια του προφήτη):

$$U_f|x\rangle = (-1)^{f(x)}|x\rangle$$

(Παρατηρούμε ότι η ιδιοτιμή για τα αντικείμενα στη λίστα που ψάχνουμε είναι -1, ενώ για αυτά που δεν ψάχνουμε +1. Αντιστρέφει, δηλαδή, το πλάτος πιθανότητας μόνο των αντικειμένων που ψάχνουμε.)

2. Εφαρμόζουμε τον μετασχηματισμό Hadamard:

$$H^{\otimes n}$$

3. Εφαρμόζουμε μια υπό συνθήκη μετατόπιση φάσης, στην οποία κάθε υπολογιστική βάση εκτός από την $|0\rangle$, λαμβάνει μία μετατόπιση φάσης -1.

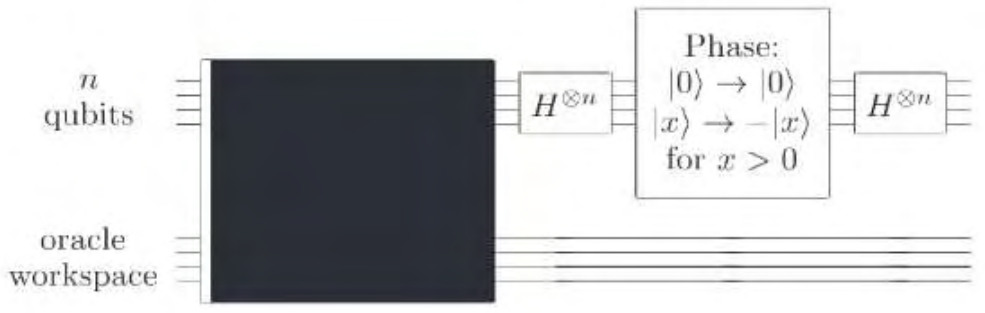
$$|x\rangle \rightarrow -(-1)^{\delta_{x0}}|x\rangle$$

Αυτό το βήμα μπορεί να εκφραστεί ισοδύναμα και από τον Τελεστή:

$$2|0\rangle\langle 0| - I$$

4. Εφαρμόζουμε τον μετασχηματισμό Hadamard:

$$H^{\otimes n}$$



Εικόνα 4.13: Κύκλωμα που εκτελεί την επανάληψη του Grover 'G' [8].

5. Το πέμπτο και τελευταίο βήμα είναι να εκτελέσουμε μια μέτρηση [8,12].

Ας αναλύσουμε το κόστος εφαρμογής μιας επανάληψης του Grover:

Βήμα 2: $\log(N)$ πράξεις

Βήμα 3: $O(n)$ κβαντικές πύλες

Βήμα 4: $\log(N)$ πράξεις

Βήμα 1: Απαιτείται μόνο μια κλήση του προφήτη και το κόστος της εξαρτάται από τις απαιτήσεις της συγκεκριμένης εφαρμογής [8,12].

Η συνολική επίδραση των βημάτων 2, 3, 4 μπορεί να περιγραφεί σε μία εξίσωση ως εξής:

$$H^{\otimes n}(|0\rangle\langle 0| - I)H^{\otimes n} = 2|\psi\rangle\langle\psi| - I \text{ , ή}$$

$$G = (2|\psi\rangle\langle\psi| - I)O$$

Όπου:

- $|\psi\rangle$ είναι η ισοπίθανη κατάσταση όλων των κβαντικών καταστάσεων που προετοιμάσαμε [8,12]

Τι κάνει, όμως, μια Επανάληψη του Grover (G);

Στην ουσία, πρόκειται για μια περιστροφή στον δισδιάστατο χώρο που παράγεται (spanned) από το αρχικό διάνυσμα $|\psi\rangle$ και την κατάσταση που αποτελείται από την ομοιόμορφη υπέρθεση των λύσεων του προβλήματος αναζήτησης [8].

Πιο αναλυτικά:

Έστω:

- Σ_x' το άθροισμα όλων των x, τα οποία αποτελούν λύσεις στο πρόβλημα αναζήτησης και
- Σ_x'' το άθροισμα όλων των x, τα οποία δεν είναι λύσεις.

Ορίζουμε επιπλέον τις κανονικοποιημένες καταστάσεις:

- $|\alpha\rangle \equiv \frac{1}{\sqrt{N-M}} \sum_x'' |x\rangle$

- $|\beta\rangle \equiv \frac{1}{\sqrt{M}} \sum'_x |x\rangle$

Άρα η αρχική κατάσταση $|\psi\rangle$, μπορεί να εκφραστεί ως:

$$|\psi\rangle \equiv \sqrt{\frac{N-M}{M}}|a\rangle + \sqrt{\frac{M}{N}}|\beta\rangle$$

και βρίσκεται στον Χώρο που παράγεται από τα διανύσματα $|\alpha\rangle$, $|\beta\rangle$.

Ας εστιάσουμε τώρα που εκφράσαμε έτσι την αρχική κατάσταση στη λειτουργία της G.
Ο προφήτης Ο προκαλεί μια αντανάκλαση γύρω από το διάνυσμα $|\alpha\rangle$ στο επίπεδο που ορίζεται από τα $|\alpha\rangle$, $|\beta\rangle$. Δηλαδή: $O(a|\alpha\rangle + b|\beta\rangle) = a|\alpha\rangle - b|\beta\rangle$
Ομοίως το $2|\psi\rangle\langle\psi| - I$ επίσης εκτελεί μια αντανάκλαση στο επίπεδο που ορίζεται από τα $|\alpha\rangle$, $|\beta\rangle$, αυτήν την φορά γύρω από το διάνυσμα $|\psi\rangle$.
Το γινόμενο δύω αντανακλάσεων, όμως, είναι μια περιστροφή!
Έτσι, η κατάσταση $G^k|\psi\rangle$ παραμένει στον χώρο που παράγεται από τα διανύσματα $|\alpha\rangle$, $|\beta\rangle$, για όλα α k.
Επίσης, μας δίνει την γωνία περιστροφής!
Έστω:

- Cos(θ/2) = $\sqrt{\frac{N-M}{M}}$, άρα και:
- $|\psi\rangle \equiv \text{Cos}\left(\frac{\theta}{2}\right)|a\rangle + \sin\left(\frac{\theta}{2}\right)|\beta\rangle$

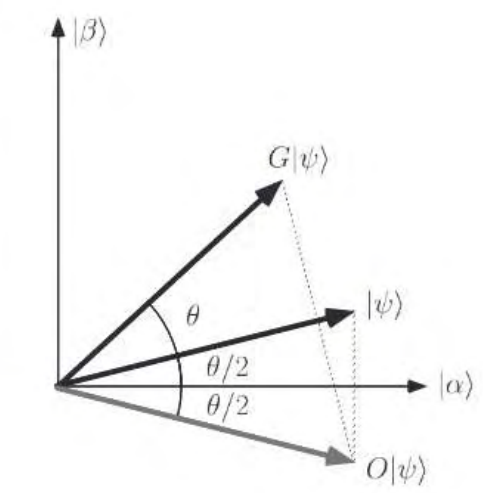
Επομένως οι δύο αντανακλάσεις που περιλαμβάνονται στην G λειτουργούν ως εξής:

$$G|\psi\rangle = \text{Cos}\left(\frac{3\theta}{2}\right)|a\rangle + \sin\left(\frac{3\theta}{2}\right)|\beta\rangle$$

και η γωνία περιστροφής είναι όντως η θ.
Επομένως η επαναλλαμβανόμενη εφαρμογή της G φέρνει την αρχική κατάσταση $|\psi\rangle$ στην κατάσταση:

$$G^k|\psi\rangle = \text{Cos}\left(\frac{2\text{k}+1}{2}\theta\right)|a\rangle + \sin\left(\frac{2k+1}{2}\theta\right)|\beta\rangle$$

Στην ουσία, η λειτουργία της G είναι η εξής: Πρόκειται για μια περιστροφή στον δισδιάστατο χώρο που παράγεται (spanned) από τα διανύσματα $|\alpha\rangle$, $|\beta\rangle$, περιστρέφοντας τον χώρο κατά θ μοίρες σε κάθε εφαρμογή της G. Η επαναλαμβανόμενη εφαρμογή της G φέρνει το διάνυσμα κατάστασης κοντά στην $|\beta\rangle$. Όταν αυτό συμβεί, μια παρατήρηση στην υπολογιστική βάση παράγει με μεγάλη πιθανότητα ένα από τα αποτελέσματα που βρίσκονται σε κατάσταση υπέρθεσης στην $|\beta\rangle$, τα οποία είναι και η λύση του προβλήματος [8].



Εικόνα 4.14: Η δράση μιας ολοκληρωμένης Επανάληψης του Grover 'G'. Πάνω στο επίπεδο που ορίζουν τα $|\alpha\rangle$, $|\beta\rangle$, αρχικά το $|\psi\rangle$ αντανακλάται γύρω από το $|\alpha\rangle$ και έπειτα γύρω από το $|\psi\rangle$, με τελική κατάσταση το διάνυσμα $G|\psi\rangle$. Αυτή η διαδικασία επαναλαμβανόμενα θα μας δώσει ένα διάνυσμα πολύ κοντά στο $|\beta\rangle$. Τότε, μια μέτρηση στην υπολογιστική βάση θα μας δώσει μια λύση στο πρόβλημα αναζήτησης με πολύ μεγάλη ακρίβεια. Μόνο $O\left(\sqrt{\frac{N}{M}}\right)$ εφαρμογές του G απαιτούνται, όπου M είναι ο αριθμός λύσεων του προβλήματος [8].

4.7 Ο αλγόριθμος του Shor

Ο αλγόριθμος του Shor για κβαντική παραγοντοποίηση πρώτων αριθμών (Shor's Quantum Factoring Algorithm), τον οποίο παρουσίασε ο Peter Shor το 1994 [13] μπορεί να λύσει προβλήματα παραγοντοποίησης μεγάλων ακεραίων αριθμών, τα οποία σε κλασσικούς υπολογιστές θα έπαιρναν αστρονομικού μεγέθους χρόνο. Αυτό, φυσικά, είναι τεράστιας σημασίας, καθώς σε αυτό το πρόβλημα βασίζεται η μέχρι τώρα κρυπτογράφηση που χρησιμοποιείται στο διαδίκτυο για ασφαλή μετάδωση δεδομένων (RSA encryption). Μια

εναλλακτική λύση, στο πρόβλημα της ασφάλειας δεδομένων στο διαδίκτυο, ενδέχεται να αποτελέσει και η κβαντική κρυπτογραφία, την οποία θα συζητήσουμε αργότερα [5].

Αν και δεν έχει αποδειχτεί ότι η παραγοντοποίηση πρώτων αριθμών δεν μπορεί να επιτευχθεί σε πολυωνυμικό χρόνο, μέχρι στιγμής δεν έχει αναπτυχθεί κάποιος αλγόριθμος που να το επιτυγχάνει. Μέχρι το 2015 ο πιο ταχύς διαθέσιμος αλγόριθμος έτρεχε σε $O\left(e^{\frac{64}{9}n^{\frac{1}{3}}(logn)^{\frac{2}{3}}}\right)$ πράξεις, όπου n είναι ο αριθμός των bit που είναι απαραίτητα για την αναπαράσταση του αριθμού που θέλουμε να παραγοντοποιήσουμε. Σε αντίθεση, ο αλγόριθμος του Shor τρέχει σε $O((logn)^2 * loglogn)$ πράξεις σε κβαντικό υπολογιστή, ακολουθούμενες από $O(logn)$ βήματα μετέπειτα επεξεργασίας σε κλασσικό υπολογιστή. Η επιτάχυνση, την οποία επιτυγχάνει, όπως παρατηρούμε, είναι εκπληκτική [14].

Συνοπτικά, ο αλγόριθμος του Shor προσπαθεί να βρει το r, η οποία είναι η περίοδος της συνάρτησης $f(a) = x^a mod\ n$, όπου το n είναι ο αριθμός που προσπαθούμε να παραγοντοποιήσουμε και x είναι ένας ακέραιος που έχει μοναδικό κοινό θετικό, ακέραιο, πρώτο παράγοντα με το n το 1 (coprime numbers).
Στο πρώτο κομμάτι βάζει τους αριθμούς που δύναται να είναι το a (όπου a διαλέγουμε ακέραιους αριθμούς στο διάστημα $[0, \dots, q-1]$, όπου ισχύει: $n^2 \leq q < 2n^2$) σε υπέρθεση στον πρώτο καταχωρητή, υπολογίζει το $x^a mod\ n$ και το τοποθετεί στον δεύτερο καταχωρητή.
Στο δεύτερο κομμάτι ο αλγόριθμος εκτελεί μέτρηση του δεύτερου καταχωρητή, η οποία προκαλεί κατάρρευση της κβαντικής μας κατάστασης σε μια συγκεκριμένη τιμή k, αλλά ταυτόχρονα φέρνει και τον πρώτο καταχωρητή σε μια κατάσταση συνεπή με τον δεύτερο (ο δεύτερος καταχωρητής περιέχει το k, ενώ ο πρώτος μια υπέρθεση καταστάσεων η οποία αν τοποθετηθεί στο a στην συνάρτηση $x^a mod\ n$, μας δίνει k).
Αφού η συνάρτηση $x^a mod\ n$ είναι περιοδική, γνωρίζουμε ότι οι τιμές που θα περιέχονται στον πρώτο καταχωρητή σε υπέρθεση θα είναι οι τιμές: $c, c+r, c+2r, \dots$, όπου c είναι ο μικρότερος ακέραιος για τον οποίο $x^c mod\ n = k$.
Στη συνέχεια ο αλγόριθμος εκτελεί QFT μετασχηματισμό στα περιεχόμενα του πρώτου καταχωρητή. Αυτό έχει ως αποτέλεσμα την ενίσχυση των πλατών πιθανότητας του πρώτου

καταχωρητή για ακέραια πολλαπλάσια του q/r.
Έπειτα μια μέτρηση στον πρώτο καταχωρητή μας δίνει ένα ακέραιο πολλαπλάσιο της αντίστροφης περιόδου.
Τέλος, το αποτέλεσμα της τελευταίας μέτρησης το παίρνει ένας κλασσικός υπολογιστής, ο οποίος κάνει μια εικασία για την πραγματική τιμή του r, και από αυτό να υπολογίσει τους πιθανούς παράγοντες του n [14]. Αυτό το τελευταίο κομμάτι της μετα-επεξεργασίας θα αναλυθεί και αργότερα.

Πιο αναλυτικά, τα βήματα του αλγορίθμου του Shor είναι τα εξής:

1. Ελέγχουμε αν το n είναι πρώτος αριθμός, ή ζυγός αριθμός, ή ακέραια δύναμη κάποιου πρώτου αριθμού. Αν είναι, είναι προτιμότερο να χρησιμοποιήσουμε μια ήδη υπάρχουσα διαδικασία σε κλασσικό υπολογιστή που καθορίζει αποδοτικά τους παράγοντές του n.
   *Βήμα που εκτελείται σε κλασσικό υπολογιστή.

2. Διαλέγουμε έναν τυχαίο αριθμό q, έτσι ώστε: $n^2 \leq q < 2n^2$
   *Βήμα που εκτελείται σε κλασσικό υπολογιστή.

3. Διαλέγουμε έναν τυχαίο αριθμό x, ο οποίος είναι σχετικά πρώτος αριθμός με το n (coprime).
   *Βήμα που εκτελείται σε κλασσικό υπολογιστή.

4. Φτιάχνουμε έναν κβαντικό καταχωρητή και τον χωρίζουμε σε δύο. Ο καθένας θα πρέπει να έχει αρκετά qubit ώστε να αποθηκεύσει ακεραίους μεγέθους εώς q-1 και n-1 αντίστοιχα.
   *Οι υπολογισμοί ως προς το πόσα qubit απαιτούνται γίνονται σε κλασσικό υπολογιστή.

5. Αρχικοποιούμε τον πρώτο καταχωρητή με την κατάσταση υπέρθεσης όλων των πιθανών καταστάσεων. Αρχικοποιούμε τον δεύτερο καταχωρητή με μηδενικά. Η συνολική κατάσταση του συστήματός μας είναι:

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|\alpha,0\rangle$$

6. Εφαρμόζουμε τον μετασχηματισμό $x^a mod\ n$ για κάθε αριθμό αποθηκευμένο στον πρώτο καταχωρητή και αποθηκεύουμε το αποτέλεσμα στον δεύτερο καταχωρητή, μέσω της χρήσης της κατάστασης υπέρθεσης που ήδη έχουμε δημιουργήσει. Η συνολική κατάστασή μας τώρα είναι:

$$\frac{1}{\sqrt{q}}\sum_{a=0}^{q-1}|\alpha,x^a mod\ n\rangle$$

7. Μετράμε τον δεύτερο καταχωρητή, από την οποία μέτρηση θα λάβουμε ως αποτέλεσμα κάποια τιμή k.

   Αυτό το βήμα έχει ως παράπλευρη επίδραση την κατάρρευση του πρώτου καταχωρητή σε μια κατάσταση υπέρθεσης όλων των τιμών $a \in [0, q-1]$, έτσι ώστε:

$$x^a mod\ n = k$$

   Η συνολική κατάσταση του συστήματος τώρα γίνεται:

$$\frac{1}{\sqrt{||A||}}\sum_{a'=a'\in A}|a',k\rangle$$

   Όπου A είναι ένα σύνολο που περιέχει τα a', έτσι ώστε $x^a mod\ n = k$ και $||A||$ ο αριθμός των στοιχείων σε αυτό το σύνολο.

8. Υπολογίζουμε τον QFT στον πρώτο καταχωρητή.

   Το αποτέλεσμα της εφαρμογής του QFT σε μια κατάσταση $|\alpha\rangle$ υπενθυμίζουμε ότι είναι το εξής:

$$QFT|a\rangle \equiv \frac{1}{\sqrt{q}}\sum_{c=0}^{q-1}e^{\frac{2\pi iac}{q}}|a\rangle$$

   Η συνολική κατάσταση του συστήματος των δύο καταχωρητών γίνεται η:

$$\frac{1}{\sqrt{||A||}} \sum_{a' \in A} \frac{1}{\sqrt{q}} \sum_{c=0}^{q-1} |c, k\rangle * e^{\frac{2\pi i a' c}{q}}$$

9. Κάνουμε μέτρηση της κατάστασης του πρώτου καταχωρητή και αποκαλούμε την τιμή που παίρνουμε m. Η τιμή m έχει πολύ μεγάλη πιθανότητα να είναι πολλαπλάσιο του $\frac{q}{r}$ (το οποίο μπορεί να επιβεβαιωθεί με την επανάληψη του αλγορίθμου εώς εδώ μερικές φορές), όπου r είναι η επιθυμητή περίοδος.
10. Παίρνουμε την τιμή m και κάνουμε κάποια μεταεπεξεργασία σε κλασσικό υπολογιστή, η οποία υπολογίζει το r, εν γνώσει των m και q. Συγκεκριμένα:
    - Το m έχει μεγάλη πιθανότητα να είναι: $m = \lambda * \frac{q}{r}$, όπου λ είναι κάποιος ακέραιος πραγματικός αριθμός.
    - Πραγματοποιούμε διαίρεση κινητής υποδιαστολής (floating point division) στο $\frac{m}{q}$ και έπειτα υπολογίζουμε την καλύτερη λογική προσέγγιση του $\frac{m}{q}$, της οποίας ο παρανομαστής είναι $\leq q$.
    - Παίρνουμε τον παρανομαστή ως υποψήφιο για την τιμή r.
    - Αν ο υποψήφιός μας είναι περιττός, τον διπλασιάζουμε αν κάτι τέτοιο οδηγεί σε τιμή $\leq q$ ή διαλέγουμε έναν νέο τυχαίο αριθμό q, και επιστρέφουμε στο βήμα 2.

    *Το βήμα αυτό εκτελείται σε κλασσικό υπολογιστή

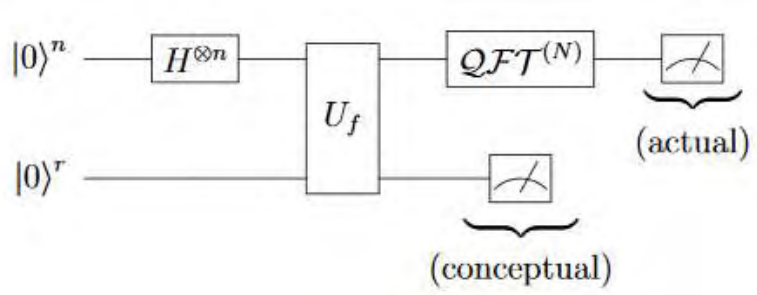
Τέλος, από την στιγμή που έχουμε το r, ένας παράγοντας του n μπορεί να καθοριστεί παίρνοντας τον ΜΚΔ (μέγιστο κοινό διαιρέτη) των $(x^{\frac{r}{2}} + 1, n)$ και ένας παίρνοντας τον ΜΚΔ των $(x^{\frac{r}{2}} - 1, n)$. Ο πολλαπλασιασμός αυτόν τον πρώτων παραγόντων μας δίνει επιτυχώς τον αριθμό n.

Σε αυτό το σημείο αν έχουμε βρει έναν πρώτο παράγοντα του n σταματάμε, αλλιώς πηγαίνουμε στο βήμα 4 (σε κάποιες συγκεκριμένες περιπτώσεις μπορεί ο αλγόριθμος του

Shor να αποτύχει, για αυτό και χρειάζεται αυτό το διορθωτικό βήμα) [14].

*Το βήμα αυτό εκτελείται σε κλασσικό υπολογιστή

Το κβαντικό κύκλωμα του αλγορίθμου μοιάζει ως εξής:



Εικόνα 4.15: Κυκλωματική αναπαράσταση του αλγορίθμου του Shor [5].

4.8 Κβαντική Κρυπτογραφία (Quantum Cryptography)

Η κρυπτογραφία είναι η τέχνη του να επιτρέπεις σε δύο πρόσωπα να επικοινωνούν με ιδιωτικότητα. Για να επιτευχθεί αυτό χρησιμοποιούνται κρυπτογραφικά πρωτόκολλα (κρυπτοσυστήματα). Ο ιδανικός στόχος ενός τέτοιου πρωτοκόλλου είναι τα δύο πρόσωπα να επικοινωνούν με όσο το δυνατόν μεγαλύτερη ευκολία γίνεται, ενώ ταυτόχρονα για κάποιον τρίτο να είναι οσο το δυνατόν πιο δύσκολο να «κρυφακούσει» στην συνομιλία τους [8].

Όπως παρατηρήσαμε, οι κβαντικοί υπολογιστές μπορούν να χρησιμοποιηθούν για να σπάσουν κάποια από τα καλύτερα κρυπτοσυστήματα δημοσίων κλειδιών (Public Key Cryptosystems). Ωστόσο, αξιοποιώντας τις ιδιαιτερότητες της κβαντομηχανικής και των κβαντικών υπολογιστών μπορούμε με μια διαδικασία που λέγεται κβαντική κρυπτογραφία (Quantum Cryptography) ή Κβαντική Διανομή Κλειδιών (Quantum Key Distribution) να εξασφαλίσουμε την ασφαλή διανομή ιδιωτικής πληροφορίας [8]. Την έννοια της κβαντικής κρυπτογραφίας εισήγαγε για πρώτη φορά ο Stephen Wiesner, ο οποίος έδειξε πώς να αποθηκεύσεις ή να μεταδώσεις μηνύματα, κωδικοποιώντας τα σε δύο συζηγή παρατηρήσιμα [15].

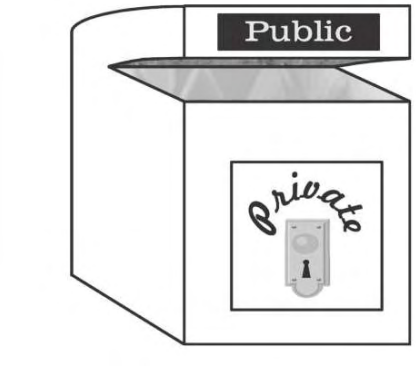
4.8.1 Κρυπτογραφία Ιδιωτικών Κλειδιών (Private Key Cryptography)

Μέχρι το 1970, όλα τα κρυπτοσυστήματα χρησιμοποιούσαν κρυπτογραφία ιδιωτικών κλειδιών. Κατά τη διάρκεια της ανταλλαγής ενός μηνύματος με την χρήση αυτής αρχής, ο πομπός και ο δέκτης πρέπει να έχουμε τα ταιριαστά κλειδιά ώστε όταν έχουν στην κατοχή τους το μήνυμα,

να το κωδικοποιήσουν ή αποκωδικοποιήσουν αντίστοιχα. Αυτή η αρχή, αν και αποδεδειγμένα πάρα πολύ ασφαλής, δεν είναι ιδιαίτερα πρακτική, λόγω του ότι απαιτούνται πάρα πολλά, μεγάλα κλειδιά (τουλάχιστον τόσο μεγάλα όσο το μέγεθος του μηνύματος), τα οποία χρησιμοποιούνται μόνο μία φορά. Επιπλέον, η διανομή των κλειδιών πρέπει να γίνει με απόλυτη ασφάλεια πριν την ανταλλαγή του ιδίου του μηνύματος, το οποίο προσθέτει επιπλέον πολυπλοκότητα στο πρόβλημα. Από το 1970 και έπειτα, τα περισσότερα κρυπτοσυστήματα χρησιμοποιούν την αρχή της Κρυπτογραφίας Δημοσίων Κλειδιών (Public Key Cryptography) [8].

4.8.2 Κρυπτογραφία Δημοσίων Κλειδιών (Public Key Cryptography) και RSA (Rivest–Shamir–Adleman)

Η πιο ακριβής και εύκολη αναλογία για να καταλάβουμε την αρχή των δημοσίων κρυπτοσυστημάτων είναι αυτή του ταχυδρομικού κουτιού.



Εικόνα 4.16: Ένα ταχυδρομικό κουτί ως αναλογία της αρχής των δημοσίων κρυπτοσυστημάτων [8].

Η ιδέα είναι ότι έχουμε ταυτόχρονα 2 κλειδιά κατά την διάρκεια μιας επικοινωνίας. Ένα ιδιωτικό, το οποίο γνωρίζει μόνο ο ιδιωκτήτης του κουτιού, με το οποίο μπορεί να αποσπάσει και να διαβάσει μηνύματα από το κουτί (αποκωδικοποίηση μηνύματος), και ένα δημόσιο κλειδί. Το δημόσιο κλειδί, το οποίο δημοσιεύεται από τον ιδιωκτήτη του κουτιού, είναι διαθέσιμο στον οποιονδήποτε και του επιτρέπει να στείλει μηνύματα στον ιδιωκτήτη του κουτιού (κωδικοποίηση μηνύματος). Έτσι, αν κάποιος τρίτος επιδιώξει να υποκλέψει την συνομιλία το μόνο που θα έχει στην διάθεσή του, θα είναι το κρυπτογραφημένο μήνυμα και το δημόσιο κλειδί, τα οποία δεν του επιτρέπουν κάπως να αποκωδικοποιήσει το μήνυμα και να το μετατρέψει σε κάποια χρήσιμη, αναγνώσιμη μορφή [8].

Αυτό που περιγράψαμε είναι η ιδανική περίπτωση. Στην πραγματικότητα, δεν έχει βρεθεί κάποιο σχήμα, το οποίο να εξασφαλίζει μαθηματικώς αποδεδειγμένα ασφαλή κρυπτογραφία δημοσίων κλειδιών. Υπάρχουν ωστόσο, τεχνικές, οι οποίες είναι ευρέως αποδεκτές ως ασφαλείς, με πιο γνωστή το κρυπτοσύστημα RSA. Αυτό, βασίζεται στην τεράστια δυσκολία που αντιμετωπίζουν οι κλασσικοί υπολογιστές στο να παραγοντοποιήσουν έναν μεγάλο αριθμό [8].

Η διαδικασία δημιουργίας κλειδιών με το κρυπτοσύστημα RSA έχει ως εξής:

1. Διαλέγουμε δύο μεγάλους πρώτους αριθμούς p, q
2. Υπολογίζουμε το γινόμενό τους $n \equiv pq$
3. Διαλέγουμε έναν τυχαίο, μικρό, πρώτο, ακέραιο αριθμό e, ο οποίος είναι σχετικά πρώτος αριθμός με την συνάρτηση:
$$\varphi(n) = (p-1)(q-1)$$
4. Υπολογίζουμε το d, το οποίο είναι το αντίστροφο ως προς την πράξη του γινομένου του e (δηλαδή $e \cdot d = 1$), mod $\varphi(n)$.
5. Το RSA δημόσιο κλειδί είναι το ζεύγος $P = (e, n)$
   Το RSA ιδιωτικό κλειδί είναι το ζεύγος $S = (d, n)$ [8]

Ας περιγράψουμε ένα ολοκληρωμένο παράδειγμα χρήσης του κρυπτοσυστήματος RSA.
Έστω ότι η Αλίκη δημιουργεί δημόσιο και ιδιωτικό κλειδί με την διαδικασία που περιγράψαμε.
Έστω τώρα ότι ένα άλλο πρόσωπο, ο Μπομπ, θέλει να χρησιμοποιήσει το δημόσιο κλειδί $P = (e, n)$ που δημιούργησε η Αλίκη, για να κρυπτογραφήσει και να στείλει το μήνυμα Μ στην Αλίκη με ασφάλεια.
Έστω ότι το μέγεθος του μηνύματος Μ είναι $\lfloor logn \rfloor$ bits (μεγαλύτερα μηνύματα μπορούν να αντιμετωπιστούν ως συλλογές από μικρότερα κομμάτια $\lfloor logn \rfloor$ bits).
Η κρυπτογράφηση ενός κομματιού του Μπομπ είναι ο υπολογισμός του:
$E(M) = M^e (mod\ n)$, όπου Ε(Μ) είναι η κρυπτογραφημένη μορφή του μηνύματος.
Τώρα η Αλίκη μπορεί να αποκυπρογραφήσει το μήνυμα Μ του Μπομπ χρησιμοποιώντας το δικό της, ιδιωτικό κλειδί, $S = (d, n)$. Αυτό γίνεται με τον υπολογισμό:

$$E(M) \rightarrow D\big(E(M)\big) = E(M)^d (mod\ n)$$

Τα δύο βασικά προβλήματα τα οποία αντιμετωπίζει το κρυπτοσύστημα RSA είναι η δημιουργία πρώτων αριθμών για την δημιουργία κλειδιών, η οποία παίρνει $O(L^4)$ πράξεις, όπου L είναι το μέγεθος του μηνύματος, και η αποδοτικότητα των μετασχηματισμός κρυπτογράφης και αποκρυπτογράφησης, οι οποίοι παίρνουν ο καθένας $O(L^3)$ πράξεις.

Υπάρχουν δύο γνωστές μέθοδοι, οι οποίες σπάνε το κρυπτοσύστημα RSA. Η μία βασίζεται στο πρόβλημα εύρεση τάξεως (order-finding) και η άλλη σε αυτό της παραγοντοποίησης πρώτων αριθμών. Και οι δύο δεν είναι εφικτές σε κλασσικό υπολογιστή καθώς ο χρόνος που απαιτούν είναι τεράστιος [8].

4.8.3 Κβαντική Διανομή Κλειδιών (Quantum Key Distribution ή QKD)

Η κβαντική διανομή κλειδιών είναι ένα μαθηματικώς αποδεδειγμένα ασφαλές πρωτόκολλο με το οποίο bits ιδιωτικών κλειδιών μπορούν να δημιουργηθούν μεταξύ δύο προσώπων χρησιμοποιώντας ένα δημόσιο κανάλι. Στη συνέχεια, τα κλειδιά αυτά μπορούν να χρησιμοποιηθούν ώστε να υλοποιηθεί ένα κλασσικό κρυπτοσύστημα ιδιωτικών κλειδιών. Για να συμβεί αυτό, πρέπει qubits να μπορούν να σταλθούν σε ένα δημόσιο κανάλι με περιθώριο λάθους κάτω από ένα κατόφλι [8].

Πώς διαφέρει αυτό το πρωτόκολλο από αυτό της κλασσικής διανομής κλειδιών;
Αυτό το πρωτόκολλο, λόγω δύο θεμελιωδών ιδιοτήτων της κβαντομηχανικής είναι απόλυτα ασφαλές. Κάποιο τρίτο πρόσωπο δεν μπορεί ποτέ να υποκλέψει πληροφορία, ακόμη και αν καταφέρει να αποκτήσει πρόσβαση στα qubit που αποστέλονται.
Οι ιδιότητες που το επιτρέπουν αυτό είναι η κατάρρευση της κυματοσυνάρτησης ενός κβαντικού συστήματος κατά τη διάρκεια της πράξης της μέτρησης και η το θεώρημα της μη-κλωνοποίησης (no-cloning theorem), το οποίο απαγορεύει την πιθανότητα κάποιος να φτιάξει το αντίγραφο μιας άγνωστης κβαντικής κατάστασης [8].

Σε αυτό το σημείο να σημειώσουμε ότι υπάρχουν πολλά πρωτόκολλα κβαντικής κρυπτογραφίας, αλλάς θα αναλύσουμε μόνο δύο. Τα BB84, E91.

4.8.4 Συνδιαλλαγή Πληροφορίας (Information Reconciliation) και Ενίσχυση Ιδιωτικότητας (Privacy Amplification)

Οι διαδικασίες συνδιαλλαγής πληροφορίας και ενίσχυσης ιδιωτικότητας είναι απαραίτητες υπορουτίνες στην ευρύτερη διαδικασία της κβαντικής κρυπτογραφίας.
Έστω ότι έχουμε δύο συσχετισμένες κλασσικές ακολουθίες bit (correlated classical bit strings) X, Y, τα οποία βρίσκονται στην κατοχή του πομπού (Αλίκη) και του δέκτη (Μπομπ) με ένα άνω όριο στην κοινή πληροφορία που κατέχει με τα X, Y ένα τρίτο πρόσωπο που προσπαθεί να υποκλέψει την συζήτηση (Eve). Με την επαναλαμβανόμενη εφαρμογή αυτών των διαδικασιών, δηλαδή την συνδιαλλαγή πληροφορίας ακολουθούμενη από την ενίσχυση ιδιωτικότητας, πετυχαίνουν την αύξηση της συσχέτισης μεταξύ των δύο ακολουθιών τους, ενώ ταυτόχρονα μειώνουν την κοινή πληροφορία της Eve με το αποτέλεσμα σε όποιο βαθμό ασφαλείας αυτοί κρίνουν αποδεκτό [8].

Η συνδιαλλαγή πληροφορίας είναι διόρθωση σφάλματος πάνω σε ένα δημόσιο κανάλι, διαδικασία η οποία συνδιαλλάσει τα σφάλματα μεταξύ των X, Y, με σκοπό να αποκτηθεί μια κοινή, αποτελούμενη ακολουθία bit W, ενώ ταυτόχρονα αποκαλύπτονται στην Eve όσο το δυνατό λιγότερα.
Μετά από αυτήν την διαδικασία, έστω ότι η Eve έχει αποκτήσει μια τυχαία μεταβλητή Z η οποία είναι μερικώς συσχετισμένη με την W.
Τώρα, εφαρμόζεται ενίσχυση ιδιωτικότητας, με την οποία αποκόπτεται από το W ένα υποσόνολο bits S, του οποίου η συσχέτιση με το Z είναι κάτω από ένα επιθυμητό κατώφλι [8].

4.9 Πρωτόκολλο BB84

Πρόκειται για το πρώτο πρωτόκολλο κβαντικής κρυπτογραφίας.
Το πρωτόκολλο, με πομπό την Αλίκη, δέκτη τον Μπομπ, και τρίτο πρόσωπο που προσπαθεί να υποκλέψει την συζήτηση την Eve, συνοψίζεται σε 9 βήματα:

1. Η Αλίκη επιλέγει $(4+\delta)n$ τυχαία bits δεδομένων a.
2. Η Αλίκη επιλέγει μία τυχαία $(4+\delta)n$-bits δυαδική ακολουθία b.
   Κωδικοποιεί κάθε bit δεδομένων του a, αντιστοιχίζοντας τα bit δεδομένων με την

ακολουθία b.

Αν το αντίστοιχο bit του b είναι 0, κωδικοποιεί κάθε bit δεδομένων ως $\{|0\rangle, |1\rangle\}$ (βάση του άξονα Z), ενώ αν το αντίστοιχο bit του b είναι 1, κωδικοποιεί κάθε bit δεδομένων ως $\{|+\rangle, |-\rangle\} = \left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$ (βάση του άξονα X).

*Σημείωση: Οι 4 καταστάσεις στις οποίες κωδικοποιεί τα bits δεδομένων δεν είναι όλες ορθωγώνιες μεταξύ τους, οπότε οποιαδήποτε μέτρηση δεν μπορεί να διαχωρίσει μεταξύ τους με βεβαιότητα. Αν, για παράδειγμα, κάνεις μια μέτρηση στη βάση Z αλλά η κατάσταση που μετρούσες ήταν μία εκ των $\left\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$, τότε η μέτρησή σου θα σου δώσει με 50% πιθανότητα την κατάσταση $|0\rangle$ και με 50% την $|1\rangle$.

3. Η Αλίκη στέλνει την κατάσταση a που προκύπτει στον Μπομπ μέσω του κβαντικού δημοσίου καναλιού επικοινωνίας.

4. Ο Μπομπ λαμβάνει $(4+\delta)n$ qubits, επηρεασμένο από την διαμεσολάβιση του καναλιού και της Eve, ανακοινώνει το γεγονός αυτό, και μετράει το κάθε qubit στη βάση του X ή Z τυχαία, ανάλογα με μία νέα τυχαία δυαδική ακολουθία b', την οποία δημιουργεί αυτός. Το αποτέλεσμά του είναι η κατάσταση a'.

   *Σημείωση: Σε αυτό το σημείο, τόσο ο Μπομπ όσο και η Eve δεν γνωρίζουν τίποτα για το b, άρα δεν μπορούν να ξέρουν σε ποια βάση πρέπει να κάνουν την μέτρηση για να πάρουν τα σωστά αποτελέσματα.

5. Η Αλίκη ανακοινώνει το b.

6. Η Αλίκη και ο Μπομπ πετάνε τα bits από τις αντίστοιχες ακολουθίες a, a' που διαθέτουν, όπου ο Μπομπ μέτρησε διαφορετική βάση από αυτήν που προετοίμασε η Αλίκη. Εκεί δηλαδή όπου τα b, b' διαφέρουν. Τα υπόλοιπα bits των a, a' είναι όμοια.
   Σε αυτό το σημείο, υπάρχει μεγάλη πιθανότητα να μείνανε τουλάχιστον 2n bits (όσο πιο μεγάλο δ επιλέξανε, τόσο μεγαλύτερη η πιθανότητα).
   Αν όχι, εγκαταλείπουμε το πρωτόκολλο.
   Αν ναι, κρατάνε και οι δύο τυχαία 2n bits.

7. Η Αλίκη διαλέγει τυχαία ένα υποσύνολο μεγέθους n bits, και λέει στον Μπομπ ποια bits διάλεξε.

8. Η Αλίκη και ο Μπομπ ελέγχουν τα n bits που επέλεξε η Αλίκη, και τα συγκρίνουν. Αν διαφέρουν παραπάνω από έναν αριθμό-κατώφλι t που έχει οριστεί, εγκεταλείπουν το πρωτόκολλο.

9. Η Αλίκη και ο Μπομπ εκτελούν αλγορίθμους συνδιαλλαγής πληροφορίας (information reconciliation) και ενίσχυσης ιδιωτικότητας (privacy amplification) στα υπολειπόμενα n bits για να αποκτήσουν m κοινά bits κλειδιού [7,8].

4.10 Πρωτόκολλο E91

Το πρωτόκολο E91 παρουσιάστηκε πρώτη φορά το 1991 από τον Artur Ekert και χρησιμοποιεί spin- ½ σωματίδια σε κατάσταση διεμπλοκής.

Τα σημεία του πρωτοκόλλου, βήμα προς βήμα, είναι τα εξής:

- Τα σωματίδια τα δημιουργεί και διανέμει στην Αλίκη (πομπός) και στον Μπομπ (δέκτη) μια πηγή. Αυτή, στέλνει κάθε φορά από ένα ζεύγος σωματιδίων σε κατάσταση διεμπλοκής.

- Υπάρχουν συγκεκριμένες διανυσματικές βάσεις μέτρησης στο πρωτόκολλο. Η βάση του άξονα X περιστραμένη κατά κάποια γωνία φ.
  Για την Αλίκη η γωνία φ παίρνει τις τιμές $\varphi_1^{\alpha} = 0°$, $\varphi_2^{\alpha} = \frac{1}{4}\pi°$, $\varphi_3^{\alpha} = \frac{1}{2}\pi°$.
  Για τον Μπομπ η γωνία φ παίρνει τις τιμές $\varphi_1^{b} = \frac{1}{4}\pi°$, $\varphi_2^{b} = \frac{1}{2}\pi°$, $\varphi_3^{b} = \frac{3}{4}\pi°$.
  Οι χρήστες διαλέγουν κάθε φορά που έρχεται καινούριο σωματίδιο την γωνία μέτρησης τυχαία και ανεξάρτητα.

- Κάθε μέτρηση μπορεί να φέρει ως αποτέλεσμα +1 (spin up) ή -1 (spin down) σε μονάδες μέτρησης $\frac{\hbar}{2}$. Αυτό ερμηνεύεται ως ένα bit πληροφορίας.

- Ορίζεται ο συντελεστής συσχέτισης των μετρήσεων των χρηστών:
  $E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j)$
  Όπου:

  - $\mathrm{P}_{\pm\pm}(\mathrm{a_i}, \mathrm{b_j})$ είναι η πιθανότητα η Αλίκη και ο Μπομπ αντίστοιχα να λάβουν ως αποτέλεσμα της μέτρησής τους ± 1 (στην βάση και γωνίας μέτρησης που τυχαία επέλεξαν).

  Σύμφωνα με τους κανόνες της Κβαντομηχανικής: $E(a_i, b_j) = -a_i \cdot b_j$

  - Όταν η Αλίκη και ο Μπομπ έχουν διαλέξει όμοιες γωνίες μέτρησης (a_2, b_1 και a_3, b_2), τότε τα αποτελέσματα των μετρήσεών τους είναι τέλεια αντίστροφα συσχετιζόμενα, δηλαδή: $E(a_2, b_1) = E(a_3, b_2) = -1$

  - Όταν η Αλίκη και ο Μπομπ έχουν διαλέξει διαφορετικές γωνίες μέτρησης (a_1, b_1 και a_1, b_3 και a_3, b_1 και a_3, b_3), τότε ορίζουμε την ποσότητα*:
    $$S = E(a_1, b_1) - E(a_1, b_3) + E(a_3, b_1) + E(a_3, b_3)$$
    Για την οποία ισχύει
    $$S = -2\sqrt{2}$$

- Όταν η μετάδοση των σωματιδίων έχει τελειώσει, η Αλίκη και ο Μπομπ ανακοινώνουν δημόσια τους προσανατολισμούς (τις γωνίες) των μετρήσεων που εκτέλεσαν για κάθε μία εκ των μετρήσεών τους και χωρίζουν τις μετρήσεις σε δύο ομάδες.
  Στην $\mathrm{G_d}$ ομάδα, η οποία περιέχει τα αποτελέσματα που έλαβαν όταν έκαναν χρήση διαφορετικής βάσης.
  Στην $\mathrm{G_k}$ ομάδα, η οποία περιέχει τα αποτελέσματα μέτρησης κατά τα οποία χρησιμοποίησαν ίδια βάση μέτρησης.

- Ανακοινώνουν οι χρήστες τα αποτελέσματα της ομάδας $\mathrm{G_d}$.
  Έπειτα, υπολογίζουν την τιμή του S.

  - Αυτή, αν δεν υπήρχε διατάραξη των σωματιδίων, θα πρέπει να έχει την τιμή: $S = -2\sqrt{2}$.

Τότε, μπορούν να γνωρίζουν ότι οι τιμές των υπολοίπων αποτελεσμάτων τους είναι τέλεια αντίστροφα συσχετιζόμενες και να τις αξιοποιήσουν για να κατασκευάσουν μια δυαδική ακολουθία – κλειδί, η οποία είναι μυστική και ασφαλής.

- Σε διαφορετική περίπτωση συμπεραίνουν ότι το κβαντικό κανάλι επικοινωνίας δεν είναι ασφαλές και τερματίζουν το πρωτόκολλο [16].

*Να σημειώσουμε σε αυτό το σημείο ότι ο τύπος από τον οποίο προκύπτει η ποσότητα S, μπορεί να τροποποιηθεί κατάλληλα, προκειμένου να αντιμετωπιστεί μια διαφορετική τεχνική διείσδυσης, όπου η ίδια η Eve (τρίτο πρόσωπο που προσπαθεί να υποκλέψει την συζήτηση) επιδιώκειι αντικαταστήσει τα δεδομένα εισόδου με δικά της [16].

ΚΕΦΑΛΑΙΟ 5

Κβαντικά Σφάλματα (Quantum Errors)

5.1 Κβαντικός Θόρυβος (Quantum Noise)

Μέχρι στιγμής ασχολούμασταν με κλειστά κβαντικά συστήματα, δηλαδή συστήματα που δεν έχουν ανεπιθύμητες αλληλεπιδράσεις με το περιβάλλον. Στον πραγματικό, φυσικό κόσμο, τέτοια συστήματα δεν υπάρχουν. Τα πραγματικά συστήματα υποφέρουν από τέτοιες αλληλεπιδράσεις, οι οποίες εισάγουν θόρυβο στο σύστημά μας. Για να καταφέρουμε να κατασκευάσουμε ισχυρούς επεξεργαστές κβαντικής πληροφορίες πρέπει να βρούμε έναν τρόπο να κατανοήσουμε και να ελέγξουμε αυτόν τον θόρυβο [8].

5.2 Φυσικά και Λογικά Qubit (Physical and Logical Qubits)

5.2.1 Φυσικό Qubit

Το φυσικό qubit είναι ένα φυσικό σύστημα, δηλαδή μια πραγματική φυσική, κβαντική αναπαράσταση ενός qubit (π.χ. ένα ηλεκτρόνιο με spin πάνω ή κάτω, ένα φωτόνιο με πόλωση οριζόντια ή κάθετη).

Η κατανόηση του πόσο ευαίσθητες είναι οι καταστάσεις των φυσικών qubit μας οδήγησε στην ανάπτυξη της κβαντικής διόρθωσης σφάλματος (quantum error correlation). Αυτό επιτυγχάνεται με την διανομή της πληροφορίας που περιέχουν σε έναν μεγάλο αριθμό φυσικών συστημάτων [17].

5.2.2 Λογικό Qubit

Το λογικό qubit είναι μια προγραμματιστική έννοια. Είναι ένα qubit το οποίο μπορεί να έχει φυσική ή αυθαίρετη υπόσταση, και εξυπηρετεί τις ανάγκες του κβαντικού αλγορίθμου που εξετάζουμε (π.χ. θα μπορούσε να προσομοιωθεί σε έναν κλασσικό υπολογιστή).

Ένα λογικό qubit μπορεί να αποτελείται από έναν μεγάλο αριθμό φυσικών qubit, κυρίως για τις ανάγκες κβαντικής διόρθωσης σφάλματος [18].

5.3 Είδη κβαντικών σφαλμάτων που μπορεί να εισάγει το περιβάλλον στο σύστημα

5.3.1 Δυαδική Αντιστροφή (Bit-Flip)

$$|0\rangle \rightarrow |1\rangle$$

$$|1\rangle \rightarrow |0\rangle$$

Πρόκειται για μια αντιστρεπτή διαδικασία, επομένως ένα τέτοιο σφάλμα μπορεί να διορθωθεί σχετικά εύκολα.

Ο μετασχηματισμός στον οποίο αντιστοιχεί ορίζεται από την πύλη X [8].

5.3.2 Αντιστροφή Φάσης (Phase-Flip Error)

$$|0\rangle \rightarrow |0\rangle$$
$$|1\rangle \rightarrow -|1\rangle$$

Πρόκειται για μια αντιστρεπτή διαδικασία, επομένως ένα τέτοιο σφάλμα μπορεί να διορθωθεί σχετικά εύκολα.

Ο μετασχηματισμός στον οποίο αντιστοιχεί ορίζεται από την πύλη Z [8].

5.3.3 Αποσυσχετισμός (Decoherence)

Κβαντικός αποσυσχετισμός είναι η διαδικασία κατά την οποία η αλληλεπίδραση των καταχωρητών μας με τυχαίες μεταβλητές του περιβάλλοντος οδηγούν στην κατάρρευση της κυματοσυνάρτησης του κβαντικού μας συστήματος.

Πρόκειται για μια μη αντιστρεπτή διαδικασία και η επαναφορά του συστήματος σχεδόν αδύνατη [3].

5.3.4 Άλλα είδη σφάλματος

Όλα τα υπόλοιπα είδη σφάλματος είναι γραμμικοί συνδυασμοί ή/και γινόμενα των δύο πρώτων σφαλμάτων που αναλύσαμε [19].

5.4 Κβαντική Διόρθωση Σφάλματος (Quantum Error Correction)

5.4.1 Εισαγωγή στην Κβαντική Διόρθωση Σφάλματος

Ο θόρυβος είναι ένα μεγάλο πρόβλημα για τα συστήματα επεξεργασίας πληροφορίας. Η προσπάθειές μας είναι εστιασμένες στο να αποφύγουμε την θόρυβο εξ' ολοκλήρου, ή, εάν αυτό δεν είναι δυνατόν, να αντιμετωπίσουμε τα αποτελέσματα αυτού. Για να έχουμε ένα μέτρο σύγκρισης, οι κλασσικοί υπολογιστές, οι οποίοι θεωρούνται εξαιρετικά αξιόπιστοι, έχουν συχνότητα σφάλματος μικρότερη από 1 σφάλμα κάθε 10^{17} πράξεις [8].

Η κβαντική διόρθωση σφάλματος είναι η ιδέα να κωδικοποιήσουμε το μήνυμα, αναπαραστώντας την κβαντική πληροφορία με πλεονασμό. Έτσι, ακόμη και αν κάποια πληροφορία του αρχικού μηνύματος διεφθαρθεί από τον θόρυβο, θα υπάρχει αρκετή πληροφορία για να ανακτήσουμε ή να αποκωδικοποιήσουμε το μήνυμα, χωρίς να χαθεί καθόλου πληροφορία από το αρχικό μήνυμα [8].

Ας δούμε ένα παράδειγμα διόρθωσης σφάλματος σε έναν κλασσικό υπολογιστή:
Έστω ότι ο πομπός θέλει να στείλει το φυσικό bit 0 σε έναν δέκτη πάνω από ένα κλασσικό κανάλι επικοινωνίας. Μια πολύ απλή τεχνική είναι να στείλει 3 αντίγραφα του bit που θέλει να στείλει (δηλαδή την ακολουθία 000). Τότε, σε περίπτωση που ο δέκτης θα λάβει, λόγω κάποιου σφάλματος, την ακολουθία 001, είναι πολύ εύκολο, εφόσον η πιθανότητα σφάλματος είναι χαμηλή, ότι υπήρξε ένα σφάλμα δυαδικής αντιστροφής στο 3ο bit, και το μήνυμα που επιδίωκε να του αποσταλθεί ήταν το bit 0.
Εφόσον η αρχική πιθανότητα bit-flip είναι p, η πιθανότητα δύο ψηφία της ακολουθίας να υποστούν bit-flip είναι $p_e = 3p^2(1-p) + p^3 = 3p^2 - 2p^3$. Για να είναι η μετάδοση πιο αξιόπιστη χρησιμοποιώντας αυτήν την τεχνική πρέπει $p_e < p => p < \frac{1}{2}$.
Αυτή η τεχνική διόρθωσης σφάλματος λέγεται ψήφος πλειονότητας (majority voting).
Η τεχνική κωδικοποίησης του μηνύματος, λέγεται κώδικας επανάληψης (repetition code) [8].

5.4.2 Ο κώδικας δυαδικής αντιστροφής για 3 qubits

Τρεις ιδιότητες που προκύπτουν από την κβαντομηχανική καταστούν τη δημιουργία κώδικα κβαντικής διόρθωσης σφάλματος πιο δύσκολο από ό,τι κλασσικής:

1. Το θεώρημα μη-κλωνοποίησης
2. Τα σφάλματα είναι συνεχή
3. Η πράξη της μέτρησης καταστρέφει κβαντική πληροφορία

Έστω ότι έχουμε ένα κανάλι επικοινωνίας (bit-flip channel) στο οποίο αποστέλουμε πληροφορία ως qubits. Η πιθανότητα ένα qubit να υποστεί bit-flip είναι p και η πιθανότητα να μείνει αδιάλλαχτο είναι 1-p. Άρα, με πιθανότητα p το qubit από την κατάσταση $|\psi\rangle$ πάει στην

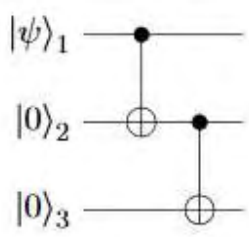
κατάσταση $X|\psi\rangle$, όπου X είναι ο τελεστής που περιγράφεται από την ήδη γνωστή x μήτρα του Pauli η οποία εκτελεί την πράξει NOT [8].

Ας περιγράψουμε τον αλγόριθμο σε 3 βήματα (Κωδικοποίηση, Ανίχνευση Σφάλματος, Διόρθωση Σφάλματος):

1. Κωδικοποιούμε τέλεια το μονό φυσικό qubit που βρίσκεται στην κατάσταση $a|0\rangle + b|1\rangle$ σε 3 λογικά qubit με κατάσταση $a|000\rangle + b|111\rangle$:

$$|0\rangle \rightarrow |0_L\rangle \rightarrow |000\rangle$$
$$|1\rangle \rightarrow |1_L\rangle \rightarrow |111\rangle$$

   Αυτό γίνεται με τη χρήση του παρακάτω κυκλώματος:

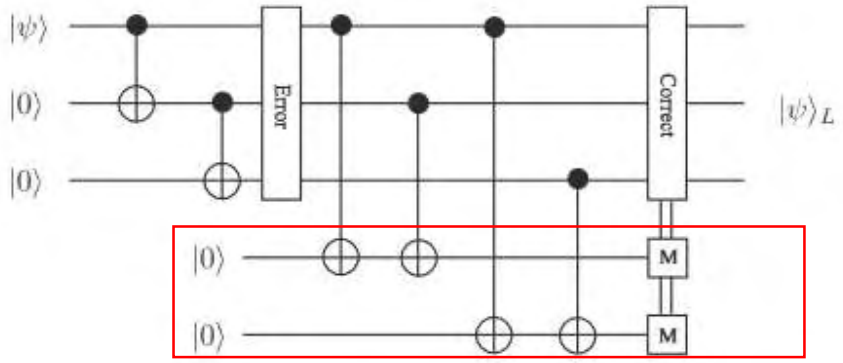


Εικόνα 5.1: Πρώτο βήμα του κώδικα δυαδικής αντιστροφής 3 qubit.
Σημείωση: Η δεύτερη CNOT πύλη μπορεί να είναι και ανάμεσα στα qubit 1,3 χωρίς καμία διαφορά [20].

   Κάθε ένα από τα 3 qubit στέλνεται μέσω ενός αξάρτητου αντίγραφου του καναλιού επικοινωνίας. Υποθέτουμε ότι υπάρχει bit-flip σφάλμα σε 1 ή λιγότερα qubits. Μπορούμε να χρησιμοποιήσουμε την ακόλουθη διαδικασία κβαντικής διόρθωσης σφαλμάτων δύο βημάτων για να ανακτήσουμε την σωστή κβαντική κατάσταση:

2. Ανίχνευση Σφάλματος / Διάγνωση Συνδρόμου (Error-Detection / Syndrome Diagnosis): Εκτελούμε μια μέτρηση για να δούμε εάν υπήρξε κάποιο σφάλμα στην κβαντική κατάσταση που αποστάλθηκε. Το αποτέλεσμα της μέτρησης λέγεται Σύνδρομο Σφάλματος (Error Syndrome). Η μέτρηση αυτή γίνεται με τη βοήθεια κάποιων επιπλέων qubit-υπηρετών (ancilla qubits).

   Το κύκλωμα που υλοποιεί αυτήν την διαδικασία φαίνεται παρακάτω:



Εικόνα 5.2: Το κύκλωμα δυαδικής αντιστροφής 3 qubit.

Τα 2 αρχικοποιημένα ancilla qubits ζευγαρώνονται με τα δεδομένα μας και έπειτα μετρώνται και μας δείχνουν εάν και πού έχει συμβεί σφάλμα στα αρχικά μας δεδομένα.

Σημείωση: Η Τρίτη C-NOT πύλη μετά το σφάλμα μπορεί να παίρνει ως control bit και το δεύτερο qubit, απλά θα πρέπει αναλόγως να αποκωδικοποιήσουμε και τα σύνδρομα σφάλματός μας [20].

Ο παρακάτω πίνακας δείχνει την κατάσταση του συστήματός μας, ακριβώς πριν την μέτρηση των ancilla qubit:

Πίνακας 5.1: Κατάσταση συστήματος πριν την μέτρηση ancilla qubit.

Error Location	Final State, $\|\text{data}\rangle \|\text{ancilla}\rangle$
No Error	$\alpha \|000\rangle \|00\rangle + \beta \|111\rangle \|00\rangle$
Qubit 1	$\alpha \|100\rangle \|11\rangle + \beta \|011\rangle \|11\rangle$
Qubit 2	$\alpha \|010\rangle \|10\rangle + \beta \|101\rangle \|10\rangle$
Qubit 3	$\alpha \|001\rangle \|01\rangle + \beta \|110\rangle \|01\rangle$

[20]

Μετά την μέτρηση, η κατάσταση του συστήματός μας καταρρέει σε μία από τις καταστάσεις που περιγράφει ο παρακάτω πίνακας, από της οποίες μπορούμε και να συμπεράνουμε ποιο από τα αρχικά μας qubit έχει υποστεί bit-flip:

Πίνακας 5.2: Τελική κατάσταση του συστήματός μας.

Ancilla Measurement	Collapsed State	Consequence
00	$\alpha \|000\rangle + \beta \|111\rangle$	No Error
01	$\alpha \|001\rangle + \beta \|110\rangle$	σ_x on Qubit 3
10	$\alpha \|010\rangle + \beta \|101\rangle$	σ_x on Qubit 2
11	$\alpha \|100\rangle + \beta \|011\rangle$	σ_x on Qubit 1

[20]

3. Ανάκτηση (Recovery):

   Χρησιμοποιούμε την τιμή του σφάλματος συνδρόμου για να μας πει ποια διαδικασία να χρησιμοποιήσουμε για να ανακτήσουμε την αρχική κατάσταση. Οι πιθανές τιμές του είναι οι ακόλουθες:

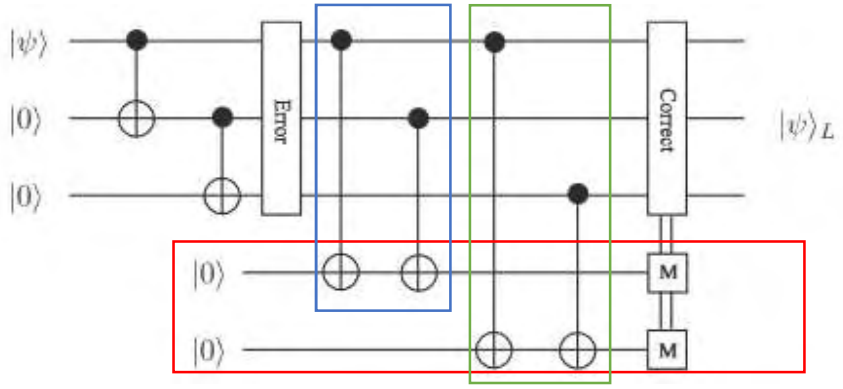
   - 00, μην κάνεις τίποτα
   - 11, έγινε bit-flip στο qubit 1, κάνε flip πάλι (εφαρμογή X_1*-gate)
   - 10, έγινε bit-flip στο qubit 2, κάνε flip πάλι (εφαρμογή X_2-gate)
   - 01, έγινε bit-flip στο qubit 3, κάνε flip πάλι (εφαρμογή X_3-gate)

Αυτή η διαδικασία λειτουργεί τέλεια, δεδομένου ότι γίνεται bit-flip σε ένα ή λιγότερα εκ των τριών qubit. Αυτό συνεπάγεται ότι όταν η πιθανότητα να γίνει bit-flip σε ένα qubit είναι $p < \frac{1}{2}$, τότε η διαδικασία που παρουσιάσαμε βελτιώνει την αξιοπιστία της κβαντικής μας κατάστασης [8,20].

*Ο δείκτης στους τελεστές X, Z, όπως για παράδειγμα X_1, Z_2 δείχνει σε ποιο qubit του συστήματός μας εφαρμόζεται ο συγκεκριμένος μετασχηματισμός.

5.4.3 Μια διαφορετική σκοπιά του κώδικα δυαδικής αντιστροφής 3 qubit

Οι δύο διαδοχικές C-NOT πύλες που εφαρμόσαμε μετά το σφάλμα στο προηγούμενο κύκλωμα, όμως, αντιστοιχούν σε κάποιους όχι και τόσο τυχαίους τελεστές, όπως θα δούμε στην συνέχεια. Οι δύο πρώτες αντιστοιχούν στον τελεστή Z_1Z_2 και οι δύο επόμενες στον τελεστή Z_2Z_3:



Εικόνα 5.3: Το κύκλωμα δυαδικής αντιστροφής 3 qubit.

Τα 2 αρχικοποιημένα ancilla qubits ζευγαρώνονται με τα δεδομένα μας και έπειτα μετρώνται και μας δείχνουν εάν και πού έχει συμβεί σφάλμα στα αρχικά μας δεδομένα [20].

- Στην ουσία, εκτελούμε δύο μετρήσεις στους τελεστές Z_1Z_2 $(Z \otimes Z \otimes I)$ και Z_2Z_3. Και οι δύο τελεστές έχουν ιδιοτιμές ± 1.

  Ο πρώτος τελεστής Z_1Z_2 μπορεί να ερμηνευτεί ως σύγκριση των δύο πρώτων qubit για να δούμε αν είναι όμοια. Αν είναι όμοια δίνει +1 και αν δεν είναι δίνει -1.

  Ο δεύτερος τελεστής Z_2Z_3 κάνει το ίδιο για qubit 2,3.

  Συγκρίνοντας τις δύο μετρήσεις συνδρόμου, μπορούμε να συμπεράνουμε με μεγάλη ακρίβεια αν και ποιο qubit έχει υποστεί δυαδική αντιστροφή.

  - $Z_1Z_2 \rightarrow +1$ & $Z_2Z_3 \rightarrow +1$: Κανένα qubit δεν υπέστει bit-flip
  - $Z_1Z_2 \rightarrow -1$ & $Z_2Z_3 \rightarrow +1$: Το 1ο qubit υπέστει bit-flip
  - $Z_1Z_2 \rightarrow +1$ & $Z_2Z_3 \rightarrow -1$: Το 3ο qubit υπέστει bit-flip
  - $Z_1Z_2 \rightarrow -1$ & $Z_2Z_3 \rightarrow -1$: Το 2ο qubit υπέστει bit-flip [8,20,22]

Καμία από τις μετρήσεις δεν μας δίνει πληροφορία για τα πλάτη πιθανότητας a, b της κωδικοποιημένης αρχικής κατάστασης και άρα, καμία από της μετρήσεις δεν προκαλεί κατάρρευση της κβαντικής μας κατάστασης, δηλαδή απώλεια πληροφορίας [8,20,22].

Αρκετή προσοχή θέλει το γεγονός ότι ο κώδικας που παρουσιάσαμε λειτουργεί μόνο για single-qubit σφάλματα, καθώς εάν συμβεί ένα bit-flip σφάλμα σε 2 qubit δεν θα μπορούμε να

εξάγουμε σαφές συμπέρασμα για το ποιο σφάλμα συνέβη από την μέτρηση του συνδρόμου σφάλματος, όπως φαίνεται από τον παρακάτω πίνακα:

Πίνακας 5.3: Πιθανά σύνδρομα σφάλματος για σφάλμα σε περισσότερα από 1 qubit.

Error	Syndrome, S	Error	Syndrome, S
$I_1 I_2 I_3$	00	$X_1 X_2 I_3$	01
$X_1 I_2 I_3$	10	$I_1 X_2 X_3$	10
$I_1 X_2 I_3$	11	$X_1 I_2 X_3$	11
$I_1 I_2 X_3$	01	$X_1 X_2 X_3$	00

[21]

5.4.4 Ο κώδικας αντιστροφής φάσης για 3 qubits

Έστω, τώρα, ότι έχουμε ένα κανάλι επικοινωνίας (bit-flip channel) στο οποίο αποστέλουμε πληροφορία ως qubits. Η πιθανότητα ένα qubit να μείνει αδιάλλαχτο είναι 1-p. Με πιθανότητα p η σχετική φάση μεταξύ των καταστάσεων $|0\rangle$ και $|1\rangle$ αντιστρέφεται. Άρα, με πιθανότητα p το qubit από την κατάσταση $|\psi\rangle$ πάει στην κατάσταση $Z|\psi\rangle$, όπου Z είναι ο τελεστής που περιγράφεται από την ήδη γνωστή z μήτρα του Pauli. Άρα μια αρχική κατάσταση $a|0\rangle + b|1\rangle$ με πιθανότητα p μετατρέπεται στην κατάσταση $a|0\rangle - b|1\rangle$ λόγω της αντιστροφής φάσης.

Τώρα μετατρέπουμε το πρόβλημα αντιστροφής φάσης σε πρόβλημα δυαδικής αντιστροφής. Δουλεύουμε στην διανυσματική βάση qubit $|+\rangle \equiv \frac{|0\rangle+|1\rangle}{\sqrt{2}}$, $|-\rangle \equiv \frac{|0\rangle-|1\rangle}{\sqrt{2}}$.
Τώρα, ο τελεστής Z, ως προς τη βάση που ορίσαμε, στέλνει την κατάσταση $|+\rangle$ στην κατάσταση $|-\rangle$ και αντίστροφα. Λειτουργεί, δηλαδή, ως τελεστής bit-flip στη βάση αυτήν.
Επομένως, θα χρησιμοποιήσουμε τις καταστάσεις $|0_L\rangle = |+++\rangle$ και $|1_L\rangle = |---\rangle$ ως καταστάσεις 0 και 1, για την προστασία εναντίον σφαλμάτων αντιστροφής φάσης.

Όλες οι διαδικασίες που περιγράψαμε και πριν (κωδικοποίηση, ανίχνευση σφάλματος, ανάκτηση), γίνονται με τον ίδιο τρόπο όπως και στην περίπτωση του bit-flip σφάλματος, απλά με βάση την $|+\rangle$, $|-\rangle$ αντί για την $|0\rangle$, $|1\rangle$. Αυτήν την μετατροπή βάσης την πετυχαίνουμε με την εισαγωγή της πύλης Hadamard και της αντίστροφής της (που είναι πάλι η ίδια) σε 2 συγκεκριμένα σημεία του κυκλώματος.

Ας περιγράψουμε πιο αναλυτικά τον αλγόριθμο:

❖ Κωδικοποίηση:

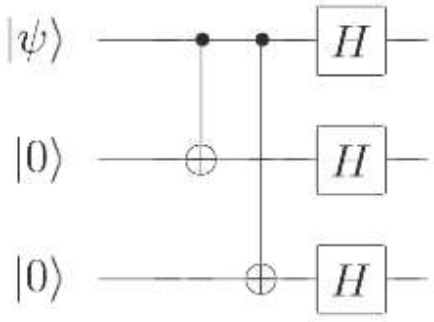
- Κωδικοποιούμε τέλεια το μονό φυσικό qubit που βρίσκεται στην κατάσταση $a|0\rangle + b|1\rangle$ σε 3 λογικά qubit με κατάσταση $a|000\rangle + b|111\rangle$ (ακριβώς όπως και στον κώδικα αντιμετώπισης αντιστροφής δυαδικού σφάλματος):

$$|0\rangle \rightarrow |0_L\rangle \rightarrow |000\rangle$$
$$|1\rangle \rightarrow |1_L\rangle \rightarrow |111\rangle$$

- Εφαρμόζουμε μια πύλη Hadamard σε κάθε λογικό qubit ξεχωριστά και παίρνουμε τις καταστάσεις:

$$|0_L\rangle \rightarrow |+++\rangle$$
$$|1_L\rangle \rightarrow |---\rangle$$

Το κύκλωμα που πετυχαίνει την κωδικοποίηση (μετρατροπή βάσης):



Εικόνα 5.4: Κύκλωμα κωδικοποίησης για τον κώδικα αντιστροφής φάσης 3 qubit [8].

❖ Ανίχνευση σφάλματος:

- Μέτρηση Συνδρόμου:

  Εφαρμόζουμε ξανά την πύλη Hadamard σε κάθε qubit, αμέσως μετά το σφάλμα (στην ουσία μετατρέψαμε το σφάλμα phase-flip σε σφάλμα bit-flip).

  Στη συνέχεια εφαρμόζουμε τις 4 διαδοχικές C-NOT πύλες, ζευγαρώνοντας τα

δεδομένα μας με τα ancilla-qubits, ακριβώς όπως και στο bit-flip σφάλμα. Αυτό, στην ουσία, ισοδυναμεί με την μέτρηση των Παρατηρήσιμων:

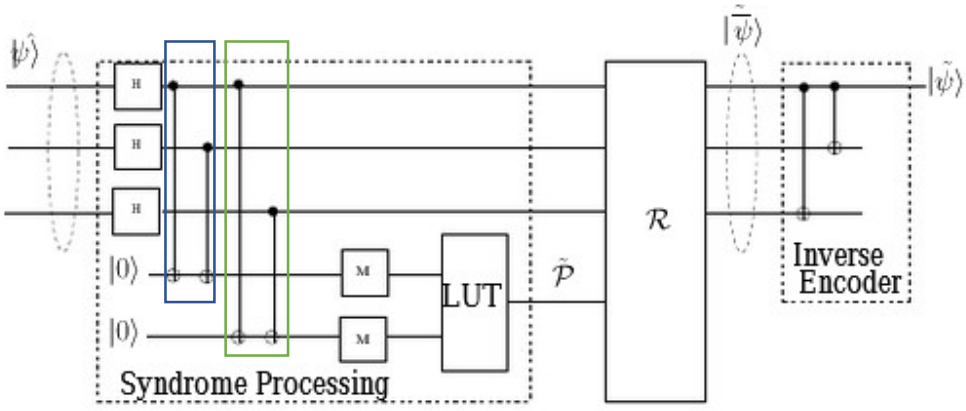
$$H^{\otimes 3} Z_1 Z_2 H^{\otimes 3} = X_1 X_2$$

$$H^{\otimes 3} Z_2 Z_3 H^{\otimes 3} = X_2 X_3$$

Αυτό ισοδυναμεί με σύγκριση των πρώτων qubit 1,2 και των qubit 2,3 αντίστοιχα. Για παράδειγμα, το $X_1 X_2$ δίνει +1 για όταν τα δύο πρώτα qubits έχουν ίδια κατεύθυνσης (π.χ. $|+\rangle, |+\rangle$) , και -1 όταν έχουν αντίθετο (π.χ. $|-\rangle, |+\rangle$). Αναλυτικά:

- $X_1 X_2 \rightarrow +1$ & $X_2 X_3 \rightarrow +1$: Κανένα qubit δεν υπέστει phase-flip
- $X_1 X_2 \rightarrow -1$ & $X_2 X_3 \rightarrow +1$: Το 1ο qubit υπέστει phase -flip
- $X_1 X_2 \rightarrow +1$ & $X_2 X_3 \rightarrow -1$: Το 3ο qubit υπέστει phase -flip
- $X_1 X_2 \rightarrow -1$ & $X_2 X_3 \rightarrow -1$: Το 2ο qubit υπέστει phase -flip

Το κύκλωμα που υλοποιεί την μέτρηση συνδρόμου, πέρα από την εισαγωγή των πυλών Hadamard, είναι ακριβώς το ίδιο με πριν:

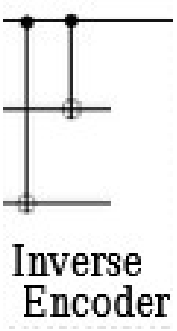


Εικόνα 5.5: Ολοκληρωμένο κύκλωμα του κώδικα αντιστροφής φάσης 3 qubit.

Με M δηλώνονται η διαδικασίες μέτρησης, LUT είναι ο Look Up Table ο οποίος δείχνει το σύνδρομο που μετράμε σε τι σφάλμα αντιστοιχεί, P δηλώνει το σφάλμα που έχει συμβεί και R (Reverse) είναι ο τελεστής ο οποίος εφαρμόζεται, ανάλογα με το σύνδρομο σφάλματος, για να διορθώσουμε το σφάλμα που προέκυψε. Inverse Encoder είναι το αντίστροφο ακριβώς κύκλωμα αυτού που χρησιμοποιούμε για την κωδικοποίηση

των qubit μας, το οποίο αντιστοιχίζει τα κωδικοποιημένα qubit μας, στην αρχική, μη κωδικοποιημένη πληροφορία μας. Π.χ. $\left|\widetilde{\psi}\right\rangle = a|000\rangle + b|111\rangle \rightarrow (a|0\rangle + b|1\rangle)|00\rangle = |\tilde{\psi}\rangle|00\rangle$ [22].

- ❖ Διόρθωση Σφάλματος:
    - Πράξη Ανάκτησης (Recovery Operation): Η πράξη ανάκτησης είναι ολόιδια με πριν. Όπου έχουμε εντοπίσει σφάλμα, αντιστρέφουμε την τιμή του συγκεκριμένου qubit, εφαρμόζοντας πύλες NOT (X-gates).
      Για παράδειγμα αν εντοπίσουμε σφάλμα αντιστροφής φάσης στο 1ο qubit, ανακτούμε την αρχική τιμή εφαρμόζοντας την πύλη X_1 στο 1ο qubit.
    - Τέλος, αν θέλουμε να καταλήξουμε στην αρχική μας πληροφορία (μη κωδικοποιημένα, αρχικά qubit), εφαρμόζουμε το αντίστροφο κύκλωμα του κωδικοποιητή, χωρίς τις πύλες Hadamard, όπως φαίνεται στην εικόνα 5.6 [8,22]:



Εικόνα 5.6: Κύκλωμα για ανάκτηση της αρχικής μας πληροφορίας στον κώδικα δυαδικής αντιστροφής 3 qubit [22].

5.4.5 Ο κώδικας Shor

Ο κώδικας Shor μπορεί να προστατέψει εναντίον τυχαίου σφάλματος σε ένα qubit και αποτελεί συνδυασμό των κωδίκων διόρθωσης σφάλματος bit-flip και phase-flip.
Οι κώδικες που κατασκευάζονται με αυτόν τον τρόπο, δηλαδή συνδυάζοντας άλλους επιμέρους κώδικες, εντάσσονται στην κατηγορία των συγκολλημένων κωδίκων (Concatenated Codes).
Ας τον περιγράψουμε σε διακριτά βήματα:

- ❖ Κωδικοποίηση:
    - Κωδικοποιούμε το φυσικό qubit όπως ακριβώς και στον phase-flip κώδικα:

$$|0\rangle \rightarrow |0_L\rangle \rightarrow |+++\rangle$$
$$|1\rangle \rightarrow |1_L\rangle \rightarrow |---\rangle$$

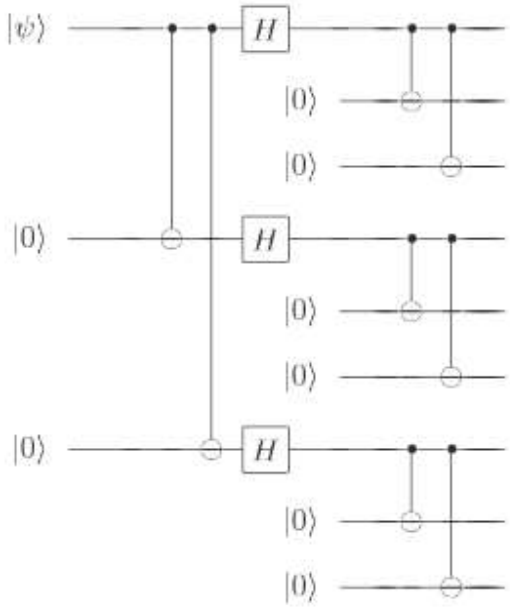
- Κωδικοποιούμε κάθε λογικό qubit όπως στον bit-flip κώδικα:

$$|+\rangle \rightarrow \frac{|000\rangle + |111\rangle}{\sqrt{2}}$$
$$|-\rangle \rightarrow \frac{|000\rangle - |111\rangle}{\sqrt{2}}$$

Δηλαδή, συνολικά:

$$|0\rangle \rightarrow |0_L\rangle \equiv \frac{(|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle) \otimes (|000\rangle + |111\rangle)}{2\sqrt{2}}$$
$$|1\rangle \rightarrow |1_L\rangle \equiv \frac{(|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle) \otimes (|000\rangle - |111\rangle)}{2\sqrt{2}}$$

Η παραπάνω διαδικασία της κωδικοποίησης υλοποιείται από το εξής κύκλωμα:



Εικόνα 5.7: Κύκλωμα κωδικοποίησης του κώδικα Shor [8].

❖ Ανίχνευση σφάλματος (για bit-flip και phase-flip σφάλματα):

- Bit-flip:

  Πραγματοποιούμε μέτρηση των Παρατηρήσιμων Z_1Z_2 και Z_2Z_3 για να συγκρίνουμε τα αντίστοιχα qubit που περιγράφονται από τους δείκτες.
  Η μέτρηση μας δίνει +1 αν είναι όμοια και -1 αν έχουν αντίθετο spin.
  Συγκρίνοντας τις δύο μετρήσεις συνδρόμου, μπορούμε να συμπεράνουμε με μεγάλη ακρίβεια αν και ποιο qubit έχει υποστεί δυαδική αντιστροφή.

  - $Z_1Z_2 \to +1$ & $Z_2Z_3 \to +1$: Κανένα qubit δεν υπέστει bit-flip
  - $Z_1Z_2 \to -1$ & $Z_2Z_3 \to +1$: Το 1ο qubit υπέστει bit-flip
  - $Z_1Z_2 \to +1$ & $Z_2Z_3 \to -1$: Το 3ο qubit υπέστει bit-flip
  - $Z_1Z_2 \to -1$ & $Z_2Z_3 \to -1$: Το 2ο qubit υπέστει bit-flip

- Phase-flip:

  Ένα σφάλμα phase-flip σε οποιοδήποτε από τα 3 λογικά qubit αλλάζει την κατάσταση ολόκληρης της πρώτης ομάδας qubit από $|000\rangle + |111\rangle$ σε $|000\rangle - |111\rangle$ και το αντίστροφο. Ομοίως και για τα λογικά qubit των άλλων ομάδων.
  Πραγματοποιούμε μέτρηση των Παρατηρήσιμων $X_1X_2X_3X_4X_5X_6$, η οποία μας δίνει +1 αν τα codewords των δύο πρώτων ομάδων qubit είναι ίδια και -1 αν διαφέρουν, και $X_4X_5X_6X_7X_8X_9$, η οποία κάνει το ίδιο για τα codewords των ομάδων 2,3.

  - $X_1X_2X_3X_4X_5X_6 \to +1$ & $X_4X_5X_6X_7X_8X_9 \to +1$: Κανένα qubit δεν υπέστει bit-flip
  - $X_1X_2X_3X_4X_5X_6 \to -1$ & $X_4X_5X_6X_7X_8X_9 \to +1$: Η 1η ομάδα υπέστει phase-flip
  - $X_1X_2X_3X_4X_5X_6 \to +1$ & $X_4X_5X_6X_7X_8X_9 \to -1$: Η 3η ομάδα υπέστει phase -flip
  - $X_1X_2X_3X_4X_5X_6 \to -1$ & $X_4X_5X_6X_7X_8X_9 \to -1$: Η 2η ομάδα υπέστει phase -flip

❖ Διόρθωση σφάλματος (για bit-flip και phase-flip σφάλματα):

- Bit-flip: Εφαρμόζουμε την πύλη X πάλι στον qubit το οποίο υπέστει bit-flip.
- Phase-flip: Ανάλογα με το ποια ομάδα υπέστει αντιστροφή εφαρμόζουμε και το αντίστοιχο παρατηρήσιμο:
  - 1η ομάδα → $Z_1Z_2Z_3$
  - 2η ομάδα → $Z_4Z_5Z_6$
  - 3η ομάδα → $Z_7Z_8Z_9$

  Τέλος, μπορούμε να αποκωδικοποιήσουμε την κατάστασή μας εφαρμόζοντας το αντίστροφο κύκλωμα από αυτό της κωδικοποίησης, για να πάρουμε την αρχική κατάσταση των τριών qubit [8,19,20,23,25].

Τώρα σε περίπτωση που έχουμε μεικτό bit-flip και phase-flip σφάλμα (π.χ. στο πρώτο qubit $Z_1X_1 = Y_1$), η διαδικασία διόρθωσης bit-flip θα διορθώσει το σφάλμα bit-flip και στη συνέχεια η διαδικασία διόρθωσης phase-flip θα διορθώσει ανεξάρτητα το σφάλμα phase-flip στην πρώτη τριπλέτα qubits. Έτσι, ο κώδικας Shor βλέπουμε ότι διορθώνει και συνδυασμούς σφαλμάτων δυαδικής και αντιστροφής φάσης, όσο αυτά συμβαίνουν σε ένα συγκεκριμένο qubit.

Για την ακρίβεια, ο κώδικας Shor, προστατεύει εναντίον τυχαίων τελείως σφαλμάτων, αρκεί να συμβαίνουν σε ένα συγκεκριμένο qubit [8,19,20,23,25].

Πώς ακριβώς γίνεται, όμως, αυτό; Πώς γίνεται να διορθώσουμε ένα τελείως τυχαίο σφάλμα;

- Έστω ότι το αρχικό μας qubit βρίσκεται στην κατάσταση $a|0\rangle + b|1\rangle$ και υφίσταται κάποιο τυχαίο σφάλμα. Η η κατάσταση που προκύπτει μπορεί να περιγραφθεί ως εξής:

$$\begin{aligned} a|0\rangle + b|1\rangle \rightarrow\ & (a|0\rangle + b|1\rangle) \otimes |A_{no\ error}\rangle_{env} \\ & + (a|0\rangle + b|1\rangle) \otimes \left|A_{bit-flip}\right\rangle_{env} \\ & + (a|0\rangle + b|1\rangle) \otimes \left|A_{phase-fli}\ \right\rangle_{env} \\ & + (a|0\rangle + b|1\rangle) \otimes |A_{both-error}\ \rangle_{env} \end{aligned}$$

Όπου $|A\rangle_{env}$ υποδηλώνει μια κατάσταση του περιβάλλοντος.

Οποιοδήποτε σφάλμα E μπορούμε να το εκφράσουμε ως γραμμικό συνδυασμό των Παρατηρήσιμων που εκφράζουν τις περιπτώσεις: μη σφάλμα (I), bit-flip σφάλμα (X), phase-flip σφάλμα (Z), bit-flip & phase-flip σφάλμα (Y):

$$E = e_1 I + e_2 X + e_3 Y + e_4 Z \ \text{[8,19,20,23,25]}$$

Τώρα, αν και η κατάσταση του qubit μπορεί να βρίσκεται σε κάποια υπέρθεση και των τεσσάρων καταστάσεων, καθώς το σφάλμα είναι στην ουσία υπέρθεση όλων των πιθανών σφαλμάτων, η μέτρηση συνδρόμου που θα κάνουμε θα το προβάλλει στη διανυσματική βάση της εξίσωσης που χρησιμοποιήσαμε. Έτσι, αναγκάζουμε το σφάλμα να καταρρεύσει σε ένα μόνο εκ των τεσσάρων σφαλμάτων. Πλέον το αποτέλεσμα της μέτρησης μας υποδεικνύει ποιον μετασχηματισμό να χρησιμοποιήσουμε (τον αντίστροφο του σφάλματος, ο οποίος ταυτίζεται με τον ίδιο).

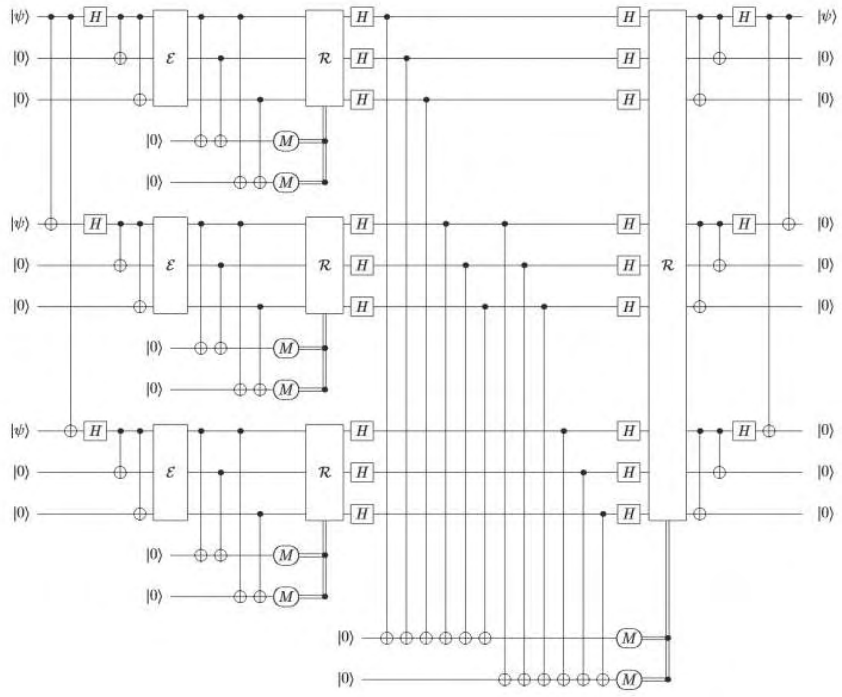
Έτσι, εφαρμόζουμε έναν εκ των τεσσάρων μετασχηματισμών:

- I
- $X \equiv \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
- $Z \equiv \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
- $Y \equiv X \cdot Z$

Εφαρμόζοντάς τον, επαναφέρουμε το qubit στην αρχική του κατάσταση.
Με αυτόν τον τρόπο, οποιοδήποτε γενικό σφάλμα μπορεί να διορθωθεί διορθώνοντας bit-flip και phase-flip σφάλματα [8,19,20,23,25].

Παρατηρούμε και επισημαίνουμε, ότι παρά το γεγονός ότι διορθώσαμε το σφάλμα, δεν έχουμε μάθει τίποτα για τους συντελλεστές a, b, καθώς κάτι τέτοιο θα οδηγούσε σε κατάρρευση της κβαντικής μας κατάστασης [8,19,20,23,25].

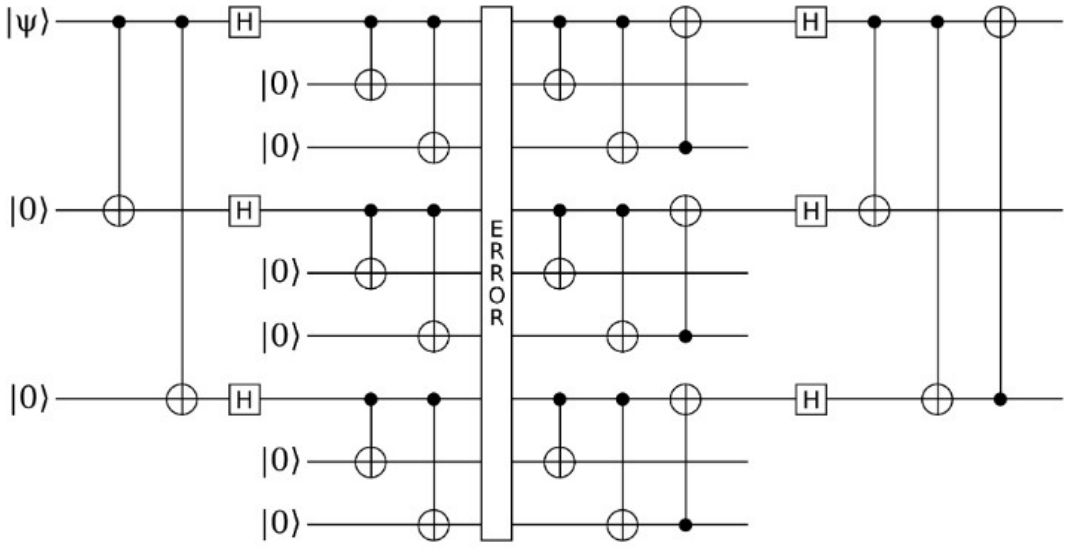
Ολόκληρο το κύκλωμα φαίνεται στην παρακάτω εικόνα:



Εικόνα 5.8: Κύκλωματική αναπαράσταση του κώδικα Shor που σχεδίασα με LaTeX.

Βασισμένο σε πληροφορίες από τις πηγές: [20-24]

Υπάρχει και το εναλλακτικό, πολύ πιο απλό κύκλωμα:



Εικόνα 5.9: Εναλλακτική κυκλωματική υλοποίηση του κώδικα Shor.

Στα αριστερά του σφάλματος, μέχρι πριν την χρήση Hadamard πυλών γίνεται η κωδικοποίηση για phase-flip και έπειτα για bit-flip και στα δεξιά γίνεται με τη σειρά αποκωδικοποίηση και διόρθωση για bit-flip μέχρι πριν την χρήση Hadamard πυλών και

τέλος αποκωδικοποίηση και διόρθωση για phase-flip.

Στο συγκεκριμένο κύκλωμα, η διαδικασία της διόρθωσης δεν μπορεί να αποσπαστεί από αυτήν της ανίχνευσης του σφάλματος [19].

5.4.6 Σταθεροποιοί κώδικες (Stabilizer Codes) C(S)

Ένας [n,k] σταθεροποιός κώδικας είναι ο διανυσματικός χώρος V(S), ο οποίος σταθεροποιείται από το υποσύνολο S του P_n , τ.ω. $-I \notin S$ και ο S έχει n-k ανεξάρτητους εναλλασσόμενους παραγωγούς $S = \langle g_1, g_2, \dots, g_{n-k} \rangle$. Τον συμβολίζουμε ως $C(S)$ [8].

Οι σταθεροποιοί κώδικες βασίζονται στην εξής τεχνική: Ενσωματώνουν qubit-υπηρέτες (ancilla qubits) σε qubit τα οποία θέλουμε να προστατέψουμε.

Χαρακτηρίζονται πλήρως από την σταθεροποιητή τους (S).

Η πιο συνήθης σύμβαση, την οποία χρησιμοποιούμε για να τους συμβολίζουμε, είναι ο συμβολισμός:

$$[[n, k, d]]$$

Όπου:

- n είναι ο αριθμός φυσικών qubit που χρησιμοποιεί ο κώδικας
- k είναι ο αριθμός λογικών qubit που χρησιμοποιεί ο κώδικας
- d είναι η απόσταση (distance) του κώδικα [8,26]

5.4.6.1 Ο Σταθεροποιός Φορμαλισμός (The Stabilizer Formalism)

Η βασική ιδέα του σταθεροποιού φορμαλισμού είναι ότι αρκετές κβαντικές καταστάσεις μπορούν να περιγραφθούν πιο εύκολα δουλεύοντας με τους τελεστές που τις σταθεροποιούν από ό,τι απευθείας με τις ίδιες.

Τι σημαίνει όμως «σταθεροποιούν»;

Για παράδειγμα η κατάσταση $|\psi\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ ικανοποιεί τις ταυτότητες:

- $X_1 X_2 |\psi\rangle = |\psi\rangle$

- $Z_1 Z_2 |\psi\rangle = |\psi\rangle$

Τότε λέμε ότι η κατάσατση $|\psi\rangle$ σταιθεροποιείται από τους τελεστές $X_1 X_2$ και $Z_1 Z_2$.
Συγκεκριμένα είναι η μοναδική κατάσταση που σταθεροποιείται από αυτούς τους τελεστές [8].

Γιατί, όμως, να χρησιμοποιήσουμε αυτόν τον φορμαλισμό;
Πολλοί κώδικες, αλλά και σφάλματα σε qubits και πράξεις περιγράφονται πιο ολοκληρωμένα με αυτόν τον φορμαλισμό, από ότι με την διανυσματική περιγραφή.

Πιο συγκεκριμένα, εάν S είναι ένα υποσύνολο του P_n και V_s το σύνολο των n κβαντικών καταστάσεων που δεν αλλάζει υπό την επίδραση των στοιχείων του S. Τότε, V_s είναι ο διανυσματικός χώρος που σταθεροποιείται από το S και S είναι ο σταθεροποιητής του V_s.
Τα στοιχεία του S πρέπει i) να μην περιέχουν τον τελεστή $-I$ και ii) να μετατίθονται (commute) [8].

Σε αυτό το σημείο εισάγουμε και την έννοια των παραγωγών:

Παραγωγοί (Generators):

Ένα σύνολο στοιχείων $g_1, g_2, \dots, g_l$ παράγει το σύνολο G εάν κάθε στοιχείο του G μπορεί να γραφεί ως γινόμενο των στοιχείων του $g_1, g_2, \dots, g_l$. Τότε, γράφουμε:
$G = \langle g_1, \dots, g_l \rangle$ [8].

5.4.6.2 Ο Σταθεροποιός Συμβολισμός και οι Μοναδιαίες Πύλες (Unitary Gates)

Ο σταθεροποιός φορμαλισμός είναι ιδιαίτερα σημαντικός στην προσπάθειά μας να περιγράφουμε την επίδραση του θορύβου και άλλων δυναμικών διαδικασιών στους κώδικές μας [8].

Αν υποθέσουμε ότι εφαρμόζουμε έναν μοναδιαίο μετασχηματισμό U σε έναν διανυσματικό χώρο V_s, ο οποίος σταθεροποιείται από το σύνολο S. $|\psi\rangle$ είναι ένα στοιχείο του V_s. Τότε, για οποιοδήποτε στοιχείο g του S ισχύει:

$$U|\psi\rangle = Ug|\psi\rangle = UgU^t U|\psi\rangle$$

Από την παραπάνω σχέση εξάγουμε τα εξής συμπεράσματα:
Η κατάσταση $U|\psi\rangle$ σταθεροποιείται από τον Τελεστή UgU^t.

Ο διανυσματικός χώρος UV_s σταθεροποιείται από την ομάδα $USU^t \equiv \{UgU^t | g \in S\}$.
Αν τα $g_1, g_2, \dots, g_l$ παράγουν το S, τότε τα $Ug_1U^t, \dots, Ug_lU^t$ παράγουν το USU^t.
Άρα για να υπολογίσουμε μια αλλαγή σε έναν σταθεροποιητή, χρειάζεται μόνο να υπολογίσουμε πώς επηρεάζονται από αυτήν την αλλαγή οι παραγωγοί του σταθεροποιητή. Αυτό είναι πολύ χρήσιμο σε συγκεκριμένες περιπτώσεις μοναδιαίων μετασχηματισμών, λόγω της βολικής μορφής των παραγωγών [8].

Σημειώνουμε ότι ισχύουν οι σχέσεις:

- $HXH^t = Z$
- $HYH^t = Y$
- $HZH^t = X$

Έτσι, σύμφωνα με την 3η εξίσωση για παράδειγμα, όταν μια πύλη Hadamard εφαρμοστεί σε μια κβαντική κατάσταση η οποία σταθεροποιείται από το Z ($|0\rangle$), τότε η κατάσταση που θα προκύψει θα σταθεροποιείται από το X ($|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$) :

$$H|0\rangle = HZ|0\rangle = HZH^tH|0\rangle = XH|0\rangle = X|+\rangle = |+\rangle$$

Έστω, τώρα, ότι είχαμε την κατάσταση $|0\rangle^{\otimes n}$, η οποία σταθεροποιείται από το σύνολο $Z_g = \langle Z_1, Z_2, \dots, Z_n\rangle$, και εφαρμόζουμε μια πύλη Hadamard σε κάθε qubit. Η κατάσταση που προκύπτει σταθεροποιείται από το σύνολο $X_g = \langle X_1, X_2, \dots, X_n\rangle$. Αυτή είναι η κατάσταση ισοπίθανης υπέρθεσης όλων των υπολογιστικών βάσεων $|\psi\rangle$:

$$H^{\otimes n}|0\rangle^{\otimes n} = H^{\otimes n}Z\,|0\rangle^{\otimes n} = H^{\otimes n}Z\left(H^{\otimes n}\right)^tH^{\otimes n}|0\rangle^{\otimes n} = XH^{\otimes n}|0\rangle^{\otimes n} = X|\psi\rangle = X\frac{1}{2^n}\sum_x|x\rangle$$

$$= |\psi\rangle = \frac{1}{2^n}\sum_x|x\rangle$$

Αξίζει να παρατηρήσουμε ότι πλέον μια κατάσταση η οποία περιγράφεται από 2^n πλάτη πιθανότητας, την περιγράψαμε χρησιμοποιώντας τους παραγωγούς $\langle X_1, X_2, \dots, X_n\rangle$ γραμμικού πλήθους n.

Αρκετοί ενδιαφέροντες μετασχηματισμοί μπορούν να εκφραστούν με παρόμοιο τρόπο, συμπεριλαμβανομένης της πύλης C-NOT με control bit το 1ο qubit και target bit το 2ο qubit και της Hadamard πύλης. Με την προσθήκη αυτών των δύο πυλών, μπορούμε πλέον να περιγράψουμε και καταστάσεις σε διεμπλοκή [8].

Το αποτέλεσμα της σύζευξης των πινάκων του Pauli με κάποιες από τις πολύ γνωστές μας πύλες δίνει τα αποτελέσματα που περιγράφονται από τον παρακάτω πίνακα:

Πίνακας 5.4: Σύζευξη των πινάκων του Pauli με γνωστές πύλες.

Operation	Input	Output
controlled-NOT	X_1	X_1X_2
	X_2	X_2
	Z_1	Z_1
	Z_2	Z_1Z_2
H	X	Z
	Z	X
S	X	Y
	Z	Z
X	X	X
	Z	$-Z$
Y	X	$-X$
	Z	$-Z$
Z	X	$-X$
	Z	Z

[8]

Για παράδειγμα, $HZH^t = X$, καθώς και θέτωντας ως U την πύλη controlled-NOT έχουμε: $UX_1U^t = X_1X_2$.
Όταν έχουμε σύζευξη με C-NOT ενός μετασχηματισμού από το σύνολο Pauli 2 qubit δρούμε ως εξής: $UX_1X_2U^t = UX_1U^tUX_2U^t = (X_1X_2)X_2 = X_1$.

Όλοι οι μοναδιαίοι μετασχηματισμοί, οι οποίοι ως σύζευξη αντιστοιχίζουν στοιχεία του G_n σε στοιχεία του G_n μπορούν να συντεθούν από πύλες Hadamard, C-NOT και Phase (S) [8].

5.4.6.3 Μετρήσεις με τον σταθεροποιό φορμαλισμό

Εκτός από την περιγραφή κάποιων μοναδιαίων μετασχηματισμών, με τον σταθεροποιό φορμαλισμό μπορούμε να εκτελέσουμε και μετρήσεις στην υπολογιστική βάση [8].

Πώς λειτουργεί αυτό;
Έστω ότι έχουμε ένα σύστημα στην κατάσταση $|\psi\rangle$ με σταθεροποιητή $\langle g_1, \dots, g_n\rangle$.

Εκτελούμε μια μέτρηση $g \in P_n$.

Πώς μετατρέπεται ο σταθεροποιητής της κατάστασής μας υπό την επίδραση μιας μέτρησης; Υπάρχουν δύο πιθανότητες:

- Ο τελεστής g μετατίθεται με όλους τους παραγώγους του σταθεροποιητή.
  - Στην πρώτη περίπτωση, μία μέτρηση του g φέρνει ως αποτέλεσμα +1 με 100% πιθανότητα.
    Η νέα κατάσταση του συστήματος είναι η $|\psi^+\rangle = \frac{(I+g)|\psi\rangle}{\sqrt{2}}$ με σταθεροποιό $\langle g, g_2, \dots, g_n \rangle$
- Ο τελεστής g αντι-μετατίθεται με έναν ή περισσότερους παραγώγους του σταθεροποιητή.
  - Στην δεύτερη περίπτωση, μία μέτρηση του g φέρνει ως αποτέλεσμα +1 με 50% πιθανότητα και -1 με 50% πιθανότητα.
    Η νέα κατάσταση του συστήματος είναι η $|\psi^-\rangle = \frac{(I-g)|\psi\rangle}{\sqrt{2}}$ με σταθεροποιό $\langle -g, g_2, \dots, g_n \rangle$ [8]

5.4.6.4 Θεωρήματα

5.4.6.4.1 Το θεώρημα Gottesman-Knill

Το θεώρημα Gottesman-Knill συνοψίζει τις δυνατότητες των σταθεροποιητών για περιγραφή μοναδιαίων διαδικασιών και μετρήσεων σε ένα κβαντικό σύστημα:

Έστω ότι πραγματοποιείται ένας κβαντικός υπολογισμός, ο οποίος περιλαμβάνει μόνο τα εξής στοιχεία:

- Προετοιμασία κβαντικών καταστάσεων στην υπολογιστική βάση
- Πύλες Hadamard, Phase, C-NOT, Pauli
- Μετρήσεις Παρατηρήσιμων του συνόλου Pauli G_n

Ένας τέτοιος υπολογισμός μπορεί να προσομοιωθεί αποδοτικά σε έναν κλασσικό υπολογιστή.

Η προσομοίωση αυτή συμβαίνει με την πιστή παρακολούθηση των παραγωγών του σταθεροποιητή, όσο συμβαίνουν διάφοροι μετασχηματισμοί κατά τη διάρκεια του κβαντικού υπολογισμού.

Το θεώρημα αποδεικνύει ότι κβαντικοί αλγόριθμοι με βελτιωμένη ταχύτητα, λόγω της δημιουργίας ζεύγων διεμπλοκής μέσω της χρήσης πυλών C-NOT και Hadamard, δεν έχουν κάποιο υπολογιστικό πλεονέκτημα, έναντι της απλής προσομοίωσής τους από κλασσικούς υπολογιστές [8].

5.4.6.4.2 Συνθήκες διόρθωσης σφάλματος για τους σταθεροποιούς κώδικες

Έστω ότι $C(S)$ είναι ο σταθεροποιός κώδικας, ο οποίος αλλοιώνεται από ένα σφάλμα $E \in P_n$.

- Όταν το E αντι-μετατίθεται με ένα στοιχείο του σταθεροποιητή το σφάλμα μεταφέρει τον $C(S)$ σε έναν ορθογώνιο υποχώρο και μπορεί να ανιχνευθεί εκτελώντας μια κατάλληλη προβολική μέτρηση.
- Αν $E \in S$, το σφάλμα δεν διαβάλλει τον χώρο μας καθόλου, οπότε δεν υπάρχει λόγος ανησυχίας.
- Όταν $E \notin S$ και μετατίθεται με όλα τα στοιχεία του S, δηλαδή: $Eg = gE$, για κάθε $g \in S$ είναι το πιο επικίνδυνο σενάριο.

Το σύνολο $E \in P_n$, για το οποίο ισχύει $Eg = gE$, για κάθε $g \in S$ είναι ο συγκεντρωτιστής (Centralizer) του S στο G_n και συμβολίζεται ως $Z(S)$.

$N(S)$ είναι ο κανονικοποιητής (Normalizer) του S, ο οποίος αποτελείται από όλα τα στοιχεία $E \in P_n$, για τα οποία ισχύει $EgE^t \in S$, για όλα τα στοιχεία $g \in S$.

Θεώρημα: *Έστω S είναι ο σταθεροποιητής για έναν σταθεροποιό κώδικα C(S).*
Έστω $\{E_j\}$ *είναι ένα σύνολο τελεστών του* G_n*, τέτοιο ώστε* $E_j^t E_k \notin N(S) - S$*, για όλα τα j,k.*
Τότε, $\{E_j\}$ *είναι το σύνολο σφαλμάτων του κώδικα C(S) που δύναται να διορθωθούν* [8].

5.4.6.5 Σημαντικοί ορισμοί σχετικά με τους σταθεροποιούς κώδικες

Σταθεροποιητής (Stabilizer) S ενός κώδικα είναι το σύνολο όλων των Pauli τελεστών M με την ιδιότητα $M|\psi\rangle = |\psi\rangle$, για όλες τις κωδικοποιημένες καταστάσεις $|\psi\rangle$ [26].
Για έναν κώδικα που κωδικοποιεί k qubits σε n, ο S έχει 2^{n-k} στοιχεία, τα οποία ονομάζονται **Παραγωγοί (generators)** [26].

Χώρος Κώδικα (Code Space) $T(S)$ ορίζεται ως ο χώρος: $T(S) = \{|\psi\rangle, \tau.\omega. M|\psi\rangle = |\psi\rangle, \forall M \in S\}$, δηλαδή ο ταυτόχρονος ιδιοχώρος με ιδιοτιμές +1 του S.
Για έναν κώδικα που κωδικοποιεί k qubits σε n, ο T(S) έχει 2^k διάσταση [26].

Η **Ομάδα Pauli (Pauli Group) P_n** είναι η ομάδα που παράγεται από τα n-τανυστικά γινόμενα των τελεστών I, X, Y, Z, όλα εξοπλισμένα με συντελεστές $\pm 1, \pm i$.
Για παράδειγμα η ομάδα G_1 αποτελείται από τα στοιχεία:
$G_1 \equiv \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\}$ [8].

Ορίζουμε **Το σύνολο $N(S) = \{N \in P_n, \tau.\omega. MN - NM, \forall M \in S)$**, δηλαδή το σύνολο όλων των τελεστών Pauli, οι οποίοι εναλλάσσονται με όλα τα στοιχεία του S. Το σύνολο αυτό λέγεται και κανονικοποιητής (Normalizer) του S [8].

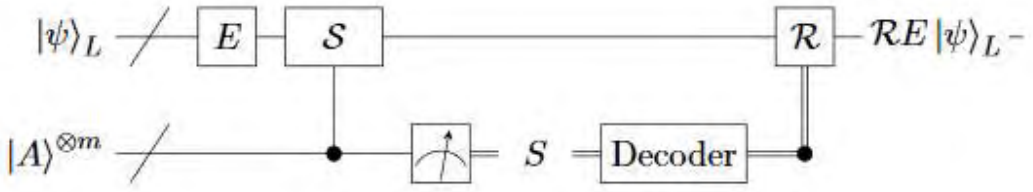
Βάρος (Weight) W ενός τελεστή Pauli $M \in P_n$ είναι ο αριθμός των qubit στα οποία ο M δρα ως μη-ταυτοτικός τελεστής. Για παράδειγμα ο τελεστής $I \otimes X \otimes Z \otimes Y$ έχει βάρος 4 [26].

Απόσταση (Distance) d ενός σταθεροποιού κώδικα είναι το βάρος του μικρότερου Τελεστή Pauli N που ανήκει στο σύνολο $N(S)\backslash S$, δηλαδή σφάλματα που είτε ανήκουν στον S είτε δεν ανήκουν στον N(S). Αυτά είναι και τα σφάλματα που ο C(S) μπορεί να ανιχνεύσει [26].

Λέξη-κωδικός (codeword) είναι μια κατάσταση $|\psi\rangle \in T(S)$, για τον χώρο κώδικα. Είναι, δηλαδή, μια κατάσταση που κωδικοποιεί τα δεδομένα μας [8].

5.4.6.6 Παραδείγματα σταθεροποιών κώδικων

Η γενική διαδικασία για επαναφορά από κάποιο σφάλμα με τη χρήση σταθεροποιών κωδίκων φαίνεται στην παρακάτω εικόνα:



Εικόνα 5.10: Γενικό κύκλωμα για διόρθωση σφάλματος με χρήση σταθεροποιών κωδίκων.
Το λογικό qubit $|\psi\rangle_L$ ενός C(S) [[n, k, d]] υφίσταται μια διαδικασία σφάλματος E.
Ένα σετ σταθεροποιητών στην συνέχεια μετριούνται με τη βοήθεια κάποιων m ancilla qubits που έχουν αρχικοποιηθεί στην κατάσταση $|A\rangle^{\otimes m}$.
Το σύνδρομο σφάλματος που προκύπτει επεξεργάζεται από έναν αποκωδικοποιητή για να αποφασίσει ποιος είναι ο κατάλληλος Τελεστής διόρθωσης που πρέπει να εφαρμοστεί για να διορθωθεί το σφάλμα που προέκυψε. Όσο πιο μεγάλος είναι ο σταθεροποιητής, τόσο πιο δύσκολη είναι η αποκωδικοποίηση του συνδρόμου.
Αφού έχει εφαρμοστεί ο κατάλληλος τελεστής, το αποτέλεσμα του κύκλου διόρθωσης σφάλματος είναι το $RE|\psi\rangle_L$.
*Οι διπλές γραμμές υποδεικνύουν ροή κλασσικής πληροφορίας [21].

Παρακάτω θα αναφέρουμε τα πιο γνωστά παραδείγματα σταθεροποιών κωδίκων. Θα παρατηρήσουμε ότι κάποιους από αυτούς ήδη τους έχουμε αναλύσει, απλά δεν γνωρίζαμε ότι ανήκουν σε αυτήν την κατηγορία και κάποιοι από αυτούς είναι τελείως καινούργιοι. Ωστόσο, δεν θα μπούμε σε πολλές λεπτομέρειες στους καινούργιους κώδικες, καθώς η κυκλωματική υλοποίησή τους είναι κάτι εξαιρετικά δύσκολο.

5.4.6.6.1 Ο κώδικας δυαδικής αντιστροφής 3 qubit

Ο ήδη γνωστός μας κώδικας δυαδικής αντιστροφής τριών qubit εκτείνεται από τις καταστάσεις $|000\rangle, |111\rangle$.

Ο σταθεροποιητής αυτής της κατάστασης είναι ο $\langle Z_1Z_2, Z_2Z_3\rangle$, που σημαίνει ότι οι παράγωγοί του είναι τα Z_1Z_2, Z_2Z_3.

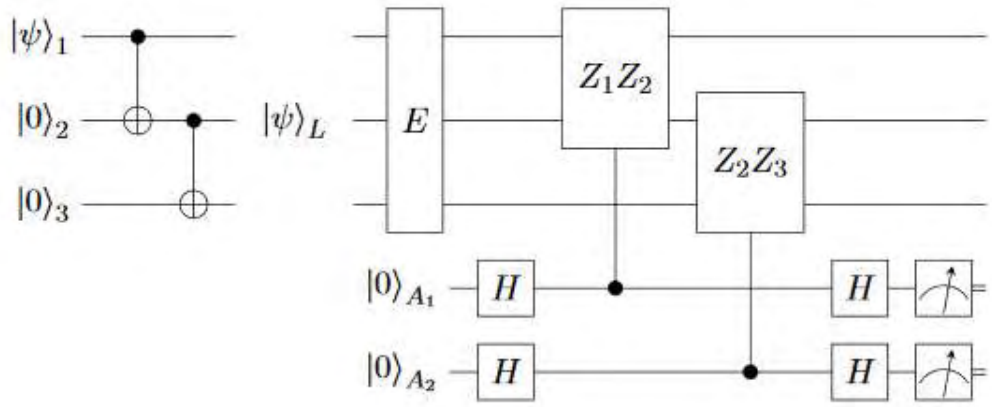
Το σύνολο το πιθανών σφαλμάτων κατά την διάγνωση συνδρόμου είναι τα $\{I, X_1, X_2, X_3\}$.

Όλα τα πιθανά γινόμενα δύο στοιχείων του συνόλου σφαλμάτων αντι-εναλλάσσονται με τουλάχιστον έναν εκ των παραγωγών του σταθεροποιητή, εκτός του I.

Έτσι, από το θεώρημα που αναπτύξαμε παραπάνω, το σύνολο $\{I, X_1, X_2, X_3\}$ σχηματίζει το σύνολο των επιδιορθώσιμων σφαλμάτων του κώδικα bit-flip τριών qubit με σταθεροποιητή το $\langle Z_1Z_2, Z_2Z_3\rangle$.

Η ανίχνευση σφάλματος γίνεται με μέτρηση των παραγωγών του σταθεροποιητή μας, Z_1Z_2, Z_2Z_3. Σε κάθε περίπτωση σφάλματος, ο σταθεροποιητής μας μετατρέπεται κατάλληλα:

- Σφάλμα: $X_1 \rightarrow$ Σταθεροποιητής: $\langle -Z_1Z_2, Z_2Z_3 \rangle$
  Αποτελέσματα μέτρησης συνδρόμου: -1, +1 .
- Σφάλμα: $X_2 \rightarrow$ Σταθεροποιητής: $\langle -Z_1Z_2, -Z_2Z_3 \rangle$
  Αποτελέσματα μέτρησης συνδρόμου: -1, -1 .
- Σφάλμα: $X_3 \rightarrow$ Σταθεροποιητής: $\langle Z_1Z_2, -Z_2Z_3 \rangle$
  Αποτελέσματα μέτρησης συνδρόμου: +1, -1 .
- Σφάλμα (όχι σφάλμα): $I \rightarrow$ Σταθεροποιητής: $\langle Z_1Z_2, Z_2Z_3 \rangle$
  Αποτελέσματα μέτρησης συνδρόμου: +1, +1 [8,21].



Εικόνα 5.11: Το κύκλωμα δυαδικής αντιστροφής 3 qubit [21].

5.4.6.6.2 Ο κώδικας Shor 9 qubit ([[9,1,3]] code)

Ο κώδικας Shor 9 qubit, τον οποίο ήδη περιγράψαμε, είναι επίσης σταθεροποιός κώδικας.

Ανήκει στην κατηγορία των CSS (Calderbank-Shor-Steane) κωδίκων, οι οποίοι είναι κώδικες που φτιάχνονται βασιζόμενοι σε ήδη υπάρχοντες κλασσικούς κώδικες, γεγονός που βοηθάει πολύ καθώς υπάρχει ήδη αρκετή γνώση από την κλασσική θεωρία κώδικα. Συγκεκριμένα, κάνουν χρήση των πινάκων ελέγχου ισότητας (parity check matrices) των κλασσικών κωδίκων, προκειμένου να κατασκευάσουν τον σταθεροποιητή τους [8.21].

*Parity Check: Η διαδικασία κατά την οποία προστίθεται ένα bit (Parity Bit ή Check Bit) στην αρχή μιας δυαδικής ακολουθίας, προκειμένου να έχουμε μόνο ή ζυγό αριθμό από bit με τιμή 1. Είναι μια από της πιο απλές μορφές κώδικα για έλεγχο σφάλματος στη μετάδωση ενός μηνύματος [27].

Έχει σταθεροποιητή S με παραγωγούς τους 8 που φαίνονται στον παρακάτω πίνακα:

Πίνακας 5.5: Σταθεροποιητής του κώδικα Shor 9 qubit.

Name	Operator
g_1	$ZZIIIIIII$
g_2	$IZZIIIIII$
g_3	$IIIZZIIII$
g_4	$IIIIZZIII$
g_5	$IIIIIIZZI$
g_6	$IIIIIIIZZ$
g_7	$XXXXXXIII$
g_8	$IIIXXXXXX$
$\bar{Z}$	$XXXXXXXXX$
$\bar{X}$	$ZZZZZZZZZ$

[8]

Οι πρώτοι 6 παραγωγοί ανιχνεύουν bit-flip σφάλματα, ενώ οι g_7, g_8 ανιχνεύουν phase-flip σφάλματα. Z, X είναι οι λογικοί τελεστές στον κώδικα.

Το σύνολο πιθανών επιδιορθώσιμων σφαλμάτων ενός qubit είναι το $\{I, X_1, X_2, X_3, X_4, X_5, X_6, X_7, X_8, X_9\}$.

Παρακάτω φαίνεται ο πίνακας με τα αποτελέσματα μέτρησης των πιθανών συνδρόμων σφαλμάτων του 9-qubit κώδικα, καθώς και το σφάλμα στο οποίο αντιστοιχούν:

Πίνακας 5.6: Πίνακας με τα σφάλματα συνδρόμου του 9 qubit κώδικα Shor.

Error	Syndrome, S	Error	Syndrome, S
X_1	10000000	Z_1	00000010
X_2	11000000	Z_2	00000010
X_3	01000000	Z_3	00000010
X_4	00100000	Z_4	00000011
X_5	00110000	Z_5	00000011
X_6	00010000	Z_6	00000011
X_7	00001000	Z_7	00000001
X_8	00001100	Z_8	00000001
X_9	00000100	Z_9	00000001

[21]

Ο κώδικας αυτός λέγεται και έκφυλος κώδικας (degenerate code), καθώς κάποια phase-flip σφάλματα μοιράζονται το ίδιο σύνδρομο σφάλματος [8,21].

Σε αυτό το σημείο να σημειώσω η κυκλωματική αναπαράσταση των δύο επόμενων κωδίκων που θα παρουσιάσουμε δεν είναι τετριμμένη και διαφέρει, ανάλογα με την ερευνητική προσέγγιση που θα ακολουθήσει κάποιος. Επίσης, όπως είδαμε και με τον κώδικα Shor, δεν υπάρχει μόνο ένας τρόπος να αναπαραστήσεις ένα κβαντικό κύκλωμα που εκτελεί κάποια λειτουργία. Για παράδειγμα μια ερευνητική ομάδα εφάρμοσε τον [[5,1,3]] κώδικα διόρθωσης σφάλματος με διαφορετικά λογικά qubit και κύκλωμα [28] από αυτά επέλεξαν κάποιες άλλες [29,30]. Παρομοίως, για τον [[7,1,3]] κώδικα διόρθωσης σφάλματος το κύκλωμα για τη μέτρηση του συνδρόμου σφάλματος μπορεί να είναι διαφορετικό [8,20,29].

5.4.6.6.3 Ο κώδικας 5 qubit ([[5,1,3]] code)

Το ελάχιστο μέγεθος ενός κώδικα που κωδικοποιεί ένα μοναδικό qubit, έτσι ώστε οποιοδήποτε σφάλμα σε ένα μοναδικό qubit στην κωδικοποιημένη κατάσταση να μπορεί να ανιχνευθεί και διορθωθεί είναι 5 qubits. Ανήκει στους κυκλικούς κώδικες, καθώς όλοι οι παραγωγοί του σταθεροποιητή του προκύπτουν με «σύρσιμο» του πρώτου κατά ένα ψηφίο δεξιά. Ο σταθεροποιητής αυτού του κώδικα φαίνεται στον επόμενο πίνακα, μαζί με τις λογικές πράξεις Z, X:

Πίνακας 5.7: Ο σταθεροποιητής του κώδικα 5 qubit και οι τελεστές Z, X.
Οι παραγωγοί g1, g4 μαζί με τους τελεστές Z, X αποτελούν το σύνολο N(S)

Name	Operator
g_1	$XZZXI$
g_2	$IXZZX$
g_3	$XIXZZ$
g_4	$ZXIXZ$
$\bar{Z}$	$ZZZZZ$
$\bar{X}$	$XXXXX$

[8]

Τα πιθανά single-qubit σφάλματα είναι το σύνολο: $\{X_1, Y_1, Z_1, X_2, Y_2, Z_2, \dots, X_5, Y_5, Z_5, I\}$

Τα λογικά qubit 0 και 1 (μία πιθανή επιλογή αυτών) είναι αντίστοιχα:

$$|0\rangle_L = \frac{1}{4}(|00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle + |00101\rangle - |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle - |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle)$$

$$|1\rangle_L = \frac{1}{4}(|11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle + |11010\rangle - |00100\rangle - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle - |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle)$$

Πρόκειται για μη-έκφυλο (non-degenerate) κώδικα, αφού χρησιμοποιεί όλα τα πιθανά σύνδρομα σφάλματος, για όλα τα πιθανά single-qubit σφάλματα, ένα προς ένα.

Και αυτός ο κώδικας μπορεί να ανιχνεύσει μόνο single-qubit σφάλματα [8,21,26,31,32].

5.4.6.6.4 Κώδικας Steane (Steane Code)

Ο κώδικας Steane χρησιμοποιείται στην κβαντική διόρθωση σφάλματος και χρησιμοποιεί 7 qubits. Μας επιτρέπει να αποθηκεύουμε την πληροφορία ενός qubit σε εφτά. Βασίζεται στον κλασσικό κώδικα διόρθωσης σφάλματος, με την ονομασία «[7,4,3] Hamming code».

Και αυτός ανήκει στην κατηγορία CSS κωδίκων. Είναι ο πιο μικρός CSS κώδικας με απόσταση 3 και είναι σημαντικός καθώς οι ιδιότητές του τον κάνουν ιδιαίτερα κατάλληλο για κβαντικούς υπολογισμούς με ανοχή στο σφάλμα (fault-tolerant quantum computations) [25].

5.4.6.6.4.1 [7,4,3] Hamming code

Κωδικοποιούμε 4 bits κλασσικής πληροφορίας (m) σε μια ομάδα των 7 bit (d). Τα υπόλοιπα 3 bits είναι τα bits ισοτιμίας (parity bits (p)).

Τα bits ισοτιμίας μπαίνουν στις θέσεις 1, 2, 4.

Τα bits δεδομένων μπαίνουν στις θέσεις 3, 5, 6, 7.

Επομένως η δυαδική μας ακολουθία μοιάζει κάπως έτσι:

$$m_7\ m_6\ m_5\ p_4\ m_3\ p_2\ p_1$$

Επομένως, υπάρχουν $2^4 = 16$ δυαδικές ακολουθίες με μήκος 7 bits που είναι έγκυρες κωδικολέξεις (codewords). Αυτές μπορούν να χαρακτηριστούν από έναν πίνακα ελέγχου ισότητας (parity check matrix):

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Κάθε έγκυρο codeword είναι μια δυαδική ακολουθία μήκους 7 bits η οποία ικανοποιεί την σχέση:

$$\sum_k H_{jk}(u_{code})_k = 0\ (mod 2)$$

Όπου:

- k είναι ο αριθμός των bit του κάθε codeword, δηλαδη $[1, \dots, 7]$.
- j είναι η γραμμή του H που παίρνουμε κάθε φορά. Παίρνει τις τιμές $1, 2, 3$.

Εάν η παραπάνω σχέση ικανοποιείται για όλες τις γραμμές του H, τότε η λέξη που παραλήφθηκε από τον δέκτη είναι αυτή που έστειλε ο πομπός χωρίς σφάλματα.
Εάν όχι, τότε έχει γίνει flip.

Εν ολίγοις, ο πολλαπλασιασμός του H με το codeword (mod2) πρέπει να δίνει την δυαδική ακολουθία 000. Αν υπάρχει κάποιο 1 σε αυτήν, έχει γίνει κάποιο bit-flip [8,25].

Η τιμή της ακολουθίας που προκύπτει από τον πολλαπλασιασμό μας υποδεικνύει ποιο bit έχει υποστεί το σφάλμα αντιστροφής.
Πώς συμβαίνει αυτό;

Τα bit (0 αν η σχέση mod2 δίνει 0; 1 αλλιώς) που προκύπτουν από την παραπάνω σχέση σχηματίζουν μια δυαδική ακολουθία, η οποία αντιστοιχίζεται σε έναν δεκαδικό αριθμό ο οποίος δείχνει σε ποιο bit έχει γίνει flip.
Για παράδειγμα αν προκύψει η ακολουθία 101, αυτό σημαίνει ότι το $5^{ο}$ bit της αρχικής ακολουθίας του δέκτη έχει γίνει flip, και χρειάζεται αντιστροφή ξανά.

Αντιστρέφουμε, λοιπόν, το bit που υποδεικνύεται, αφαιρούμε τα parity bits, και η ακολουθία που έχει πλέον ο δέκτης, είναι η σωστή, αρχική ακολουθία που έστειλε ο πομπός [8,25].

Προσοχή, η τεχνική αυτή λειτουργεί μόνο στην περίπτωση που η ακολουθία έχει υποστεί ≤ 1 bit-flips [8,25].

5.4.6.6.4.2 [[7,1,3]] Steane code

Ο κώδικας Steane γενικεύει αυτόν τον κλασσικό κώδικα διόρθωσης σφάλματος σε έναν παρόμοιο, κβαντικό κώδικα. Χρησιμοποιεί 7 qubits για να κωδικοποιήσει 1 qubit κβαντικής πληροφορίας και μας επιτρέπει να επανέλθουμε από κάποιο τυχαίο σφάλμα (τυχαίος μοναδιαίος μετασχηματισμός ή κβαντική αποσυσχέτιση) που προέκυψε σε οποιοδήποτε ένα από τα 7 qubits (σφάλμα X, σφάλμα Y ή ταυτόχρονο σφάλμα X, Y) [19,20,22,25,31,33].

Ο σταθεροποιητής αυτού του κώδικα είναι ο ακόλουθος:

Πίνακας 5.8: Σταθεροποιητής του κώδικα Steane [[7,1,3]].

M_1	σ_x	σ_x	σ_x	σ_x	I	I	I
M_2	σ_x	σ_x	I	I	σ_x	σ_x	I
M_3	σ_x	I	σ_x	I	σ_x	I	σ_x
M_4	σ_z	σ_z	σ_z	σ_z	I	I	I
M_5	σ_z	σ_z	I	I	σ_z	σ_z	I
M_6	σ_z	I	σ_z	I	σ_z	I	σ_z
$\overline{X}$	I	I	I	I	σ_x	σ_x	σ_x
$\overline{Z}$	I	I	I	I	σ_z	σ_z	σ_z

[26]

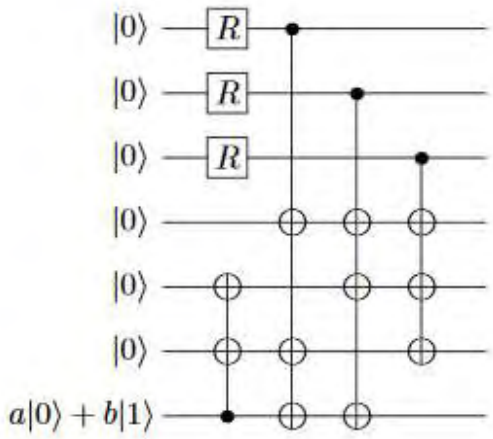
Στον κώδικα Stean [[7,1,3]] προετοιμάζουμε ως λογικό 0 την κατάσταση υπέρθεσης όλων των codeword του κλασσικού Hamming code οι οποίες έχουν ζυγό αριθμό ‘1’:

$$|0_L\rangle = \frac{1}{\sqrt{8}}(|0000000\rangle + |0001111\rangle + |0110011\rangle + |0111100\rangle + |1010101\rangle + |1011010\rangle + |1100110\rangle + |1101001\rangle)$$

Και ως λογικό 1 την κατάσταση υπέρθεσης όλων των codeword του Hamming code οι οποίες έχουν μονό αριθμό ‘1’:

$$|1_L\rangle = \frac{1}{\sqrt{8}}(|1111111\rangle + |1110000\rangle + |1001100\rangle + |1000011\rangle + |0101010\rangle + |0100101\rangle + |0011001\rangle + |0010110\rangle)$$ [25], [33], [20], VII, , [22], A, [19], 8, [31], 3

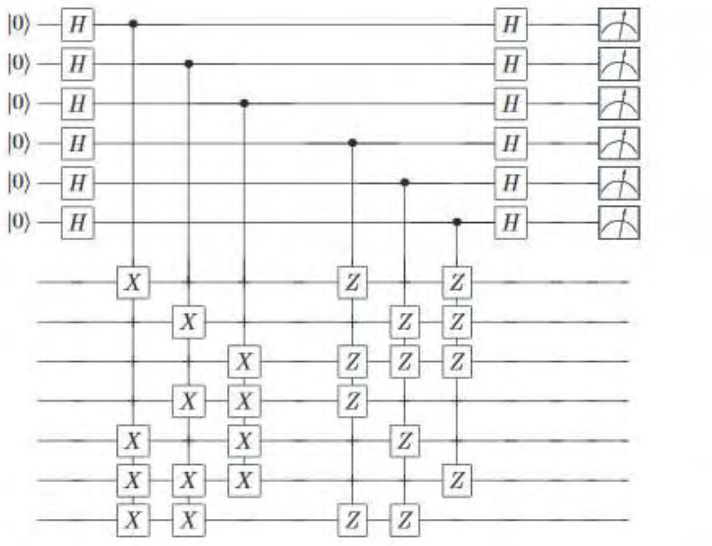
Το κύκλωμα που υλοποιεί την κωδικοποίηση μπορεί να φανεί παρακάτω:



Εικόνα 5.12: Κύκλωμα κωδικοποίησης του κώδικα Steane [[7,1,3]].

Στην συγκεκριμένη εικόνα, με το γράμμα R σημειώνονται οι πύλες Hadamard [25].

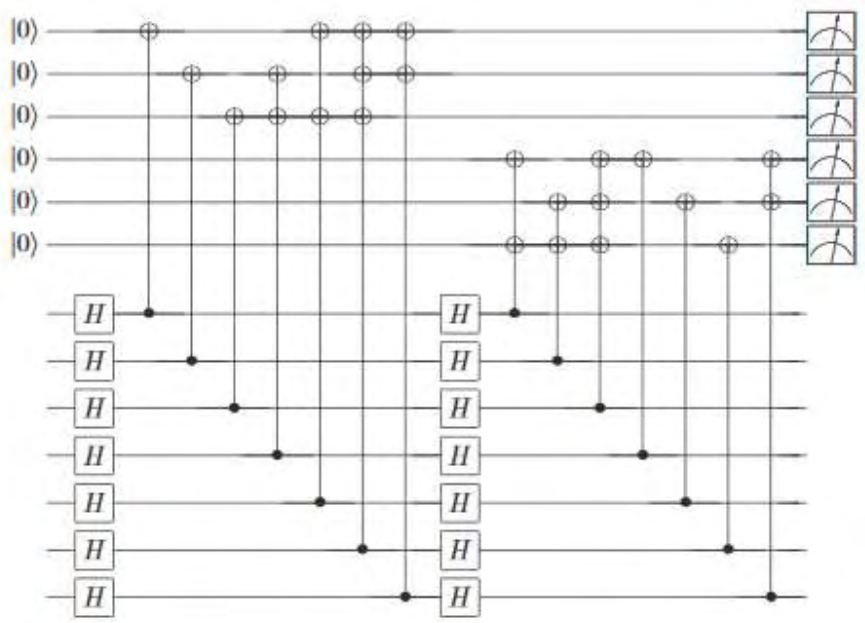
Η μέτρηση των σταθεροποιητών, δηλαδή ο εντοπισμός του συνδρόμου σφάλματος δύναται να γίνει με το ακόλουθο κύκλωμα:



Εικόνα 5.13: Κύκλωμα εντοπισμού συνδρόμου σφάλματος του κώδικα Steane [[7,1,3]].

Τα πρώτα 6 qubit είναι τα ancilla-qubits και τα επόμενα 7 είναι τα qubit δεδομένων του αλγορίθμου [8].

Το προηγούμενο κύκλωμα είναι ισοδύναμο και με το κύκλωμα:



Εικόνα 5.14: Εναλλακτικό κύκλωμα εντοπισμού συνδρόμου σφάλματος του κώδικα Steane [[7,1,3]] [8].

5.4.6.6.5 Άλλοι σταθεροποιοί κώδικες για κβαντική διόρθωση σφάλματος

Υπάρχουν και μπορούν να κατασκευαστούν και άλλοι, πολλοί σταθεροποιοί κώδικες. Για παράδειγμα στην πηγή [34], παρουσιάζεται ένας κώδικας [[8,3,5]] από μία ομάδα ερευνητών το 2012. Επίσης, υπάρχουν και άλλες οικογένειες κωδίκων, όπως για παράδειγμα οι κώδικες επιφάνειας (surface code), οι οποίοι είναι μια οικογένεια κωδίκων που ορίζονται πάνω σε δισδιάστατα πλέγματα από qubits [35,36].

Αυτά που πρέπει να προσέχουμε όταν κατασκευάζουμε έναν σταθεροποιό κώδικα είναι τα εξής:

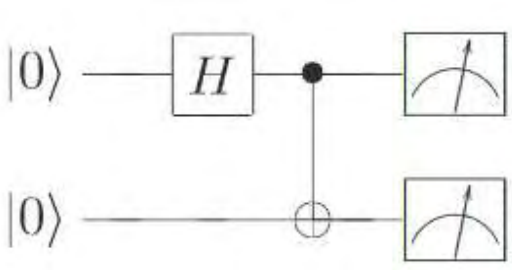
- Να έχει λίγα φυσικά qubit
- Να έχει πολλά λογικά qubit
- Να έχει μεγάλη απόσταση, δηλαδή να μπορεί να διορθώσει πολλά σφάλματα
- Να έχει καλό αλγόριθμο αποκωδικοποίησης σφάλματος συνδρόμου, μιας και το πρόβλημα αυτό γίνεται σε υπολογιστή και είναι ιδιαίτερα δύσκολο [33,37].

5.5 Κβαντικοί Υπολογισμοί με Ανοχή Σφαλμάτων (Fault-Tollerant Quantum Computation)

Η κβαντική πληροφορία, ωστόσο, δεν υφίσταται σφάλματα από τα οποία πρέπει να προστατευτούμε μόνο κατά τη διάρκεια της αποθήκευσης και μετάδοσής της, αλλά και κατά τη διάρκεια της εφαρμογής κβαντικών υπολογισμών (μετρήσεις, κβαντικές πύλες, μετάδοση μέσω κβαντικών καλωδίων). Παρά το γεγονός αυτό, αποδεικνύεται ότι τυχαία καλοί κβαντικοί υπολογισμοί μπορούν να επιτευχθούν όταν η πιθανότητα σφάλματος ανά κβαντική πύλη είναι κάτω από ένα κατώφλι [8].

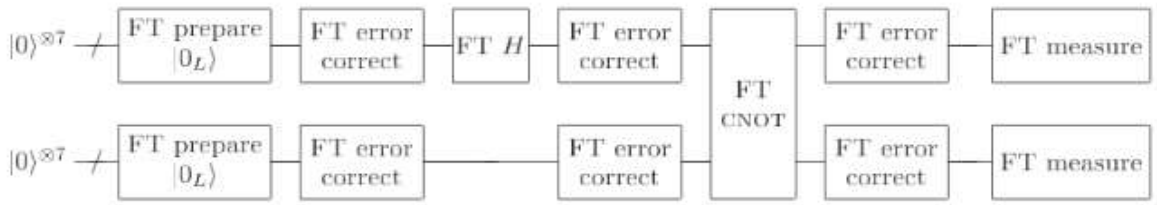
Η βασική ιδέα του κβαντικού υπολογισμού με ανοχή σφαλμάτων είναι να κάνουμε τους υπολογισμούς κατευθείαν σε κωδικοποιημένες κβαντικές καταστάσεις (quantum encoded states) με τέτοιο τρόπο ώστε να μην χρειάζεται ποτέ αποκωδικοποίηση.

Ο θόρυβος, όπως αναφέραμε και νωρίτερα, επηρεάζει όλα τα στοιχεία του κβαντικού μας κυκλώματος. Για να τον αντιμετωπίσουμε αντικαθιστούμε όλα τα αρχικά qubit με μια κωδικοποιημένη ομάδα από qubits, χρησιμοποιώντας έναν κώδικα διόρθωσης σφάλματος (π.χ. κώδικας Steane), και όλες τις κβαντικές πύλες με μια διαδικασία εφαρμογής μιας κωδικοποιημένης πύλης (encoded gate) σε μια κωδικοποιημένη κατάσταση (encoded state) [8,25].



Εικόνα 5.15: Ένα απλό κβαντικό κύκλωμα με μια πύλη CNOT.

Εάν κάθε στοιχείο του κυκλώματος αποτυγχάνει με πιθανότητα p, τότε η πιθανότητα σφάλματος στην έξοδο είναι $O(p)$ [8].



Εικόνα 5.16: Το ίδιο κύκλωμα με το παραπάνω, χρησιμοποιώντας κωδικοποιημένα qubits, πύλες και λογικές πράξεις.

Εάν χρησιμοποιούνται ανεκτικές στο σφάλμα διαδικασίες σε όλα τα βήματα, τότε η πιθανότητα σφάλματος στην έξοδο είναι

$O(p^2)$, δηλαδή μια τάξη μεγέθους μικρότερη από ότι στο προηγούμενο κύκλωμα!
Παρατηρούμε ότι εφαρμόζονται διαδικασίες διόρθωσης σφάλματος περιοδικά ακόμη και σε σημεία που δεν συμβαίνει τίποτα στο κύκλωμα, καθώς ένα σφάλμα μπορεί να προκύψει και στην μνήμη του συστήματος, χωρίς να συμβαίνει απαραίτητα κάποια διαδικασία εκείνη την στιγμή [8].

Με το να πραγματοποιούμε διόρθωση σφάλματος περιοδικά σε μια κωδικοποιημένη κατάσταση, αποτρέπουμε τη συσσώρευση σφάλματος στην κατάστασή μας. Ωστόσο, δεν αρκεί αυτό, ακόμη και αν εφαρμόζουμε διόρθωση σφάλματος μετά από κάθε κωδικοποιημένη πύλη. Πρέπει να είμαστε πολύ προσεκτικοί, καθώς:

- Οι κωδικοποιημένες πύλες ενδέχεται να διαδώσουν το σφάλμα λόγω θορύβου στα κωδικοποιημένα qubit εξόδου.
- Η διαδικασία της ίδιας της διόρθωσης σφάλματος μπορεί να εισάγει σφάλματα στα κωδικοποιημένα qubit εξόδου [8.25].

Δεν θα μπούμε σε περισσότερες λεπτομέρειες στην ανοχή σφάλματος, καθώς είναι μια εξαιρετικά περίπλοκη διαδικασία και από μόνη της θα μπορούσε να πάρει άπειρο χρόνο.

5.5.1 Κβαντικό Θεώρημα Κατωφλίου (Quantum Threshold Theorem)

Το θεώρημα κατωφλίου είναι το εξής:
Ένα κβαντικό κύκλωμα που αποτελείται από p(n) πύλες μπορεί να προσομοιωθεί με πιθανότητα σφάλματος το πολύ ε χρησιμοποιώντας:

$$O\left(poly\left(\log\left(\frac{p(n)}{\varepsilon}\right)\right)p(n)\right)$$

πύλες σε υπολογιστικό μηχάνημα του οποίου τα στοιχεία αποτυγχάνουν με πιθανότητα το πολύ p, δεδομένου ότι το p είναι χαμηλότερο από μία σταθερά κατωφλίου (threshold), $p < p_{th}$*, και δεδομένου φυσιολογικών επιπέδων θορύβου στο υπολογιστικό μηχάνημα* [8].

ΚΕΦΑΛΑΙΟ 6

Πρακτική υλοποίηση κβαντικού υπολογιστή

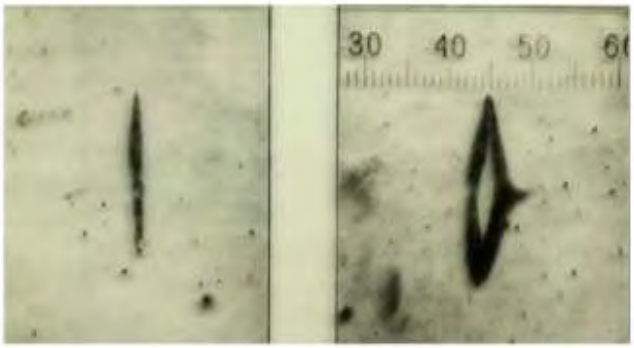
Καλή όλη η θεωρία και οι αλγόριθμοι που παρουσιάσαμε, οι οποίοι αποδεδειγμένα, θεωρητικά, λειτουργούν, αλλά για να γίνουν όλα αυτά χρήσιμα στην πράξη, πρέπει να φτιάξουμε μια συσκευή, έναν υπολογιστή που να διαχειρίζεται όλες αυτές τις ιδιότητες και να παράγει κάποια αποτελέσματα κάποιας αξίας για τον άνθρωπο. Έναν κβαντικό υπολογιστή.

6.1 Το Πείραμα Stern-Gerlach

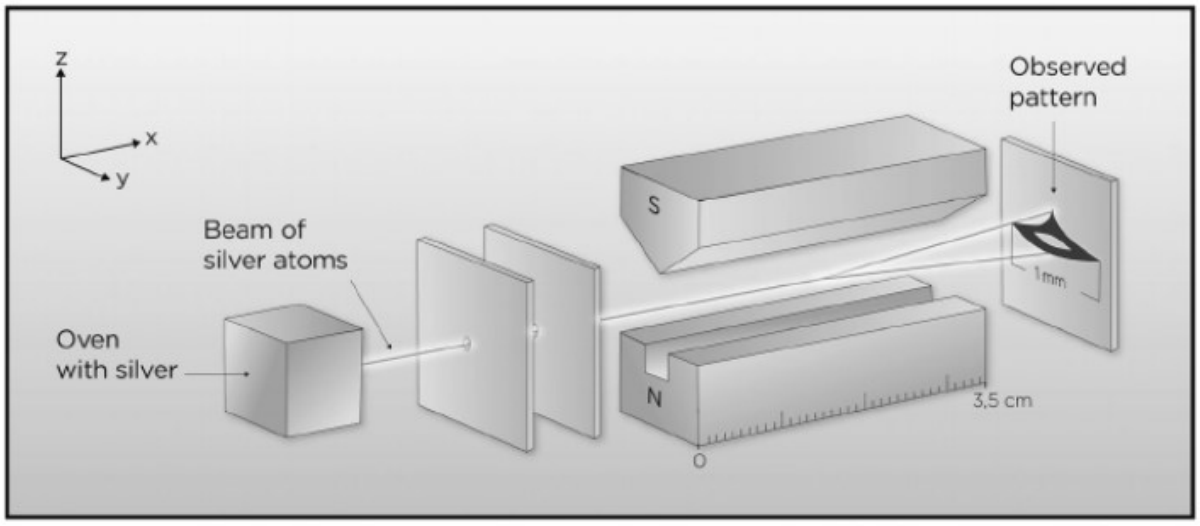
Το πείραμα Stern-Gerlach σχεδιάστηκε από τον Otto Stern το 1921 και εφαρμόστηκε από τον ίδιο και τον Walther Gerlach το 1922 [38].
Αποτέλεσε θεμέλιο λίθο στην πορεία προς την κατασκευή ενός κβαντικού υπολογιστή.

Συμπεράσματα του πειράματος: Αποτέλεσε την πρώτη πειραματική επιβεβαίωση της υπόθεσης ότι η ιδιότητα της στροφορμής, στον κβαντικό κόσμο, είναι κβαντισμένη, αλλά και έδειξε ξεκάθαρα ότι σε όλες τις κβαντικές μετρήσεις η κατευθυντική κβάντωση είναι απαραίτητη προϋπόθεση. Μέτρησε για πρώτη φορά την ιδιότητα Θεμελιώδους Κατάστασης (Ground State) ενός ατόμου και έθεσε τη βάση για την αποκάλυψη του spin του ηλεκτρονίου [7,38-40].

Περιγραφή του πειράματος:
Μία ακτίνα ατόμων αργύρου (άτομα με μη-μηδενική μαγνητική ροπή) αποστέλεται μέσω ενός ανομοιογενούς μαγνητικού πεδίου και παρατηρείται η εκτροπή της. Μέχρι τότε, σύμφωνα με την Κλασσική Φυσική, κάποιος θα περίμενε οι μαγνητικές στιγμές των ατόμων σιδήρου να κατευθυνθούν τυχαία, καθώς ανάλογα με τον προσανατολισμό τους θα εκτρέπονταν από το ανομοιογενές μαγνητικό πεδίο κατά ένα διαφορετικό ποσοστό. Ωστόσο, οι ερευνητές παρατήρησαν ότι η ακτίνα δισπάστηκε σε δύο πιθανές καταστάσεις, οι οποίες αργότερα ονομάστηκαν spin up και spin down [7,38-40].



Εικόνα 6.1: Πραγματικά αποτελέσματα του πειράματος SGE. Το αριστερά είναι το αποτέλεσμα χωρίς την χρήση ανομοιογενούς πεδίου, το δεξιά με τη χρήση ενός μαγνητικού πεδίου. Επειδή η ισχύς του ανομοιογενούς πεδίου μειώνεται ταχεία όσο απομακρυνόμαστε από την άκρη του μαγνήτη, οι συνιστώσες της ακτίνας ενώνονται [39].



Εικόνα 6.2: Αναπαράσταση του SGE.

Οι πλάκες μετά τον φούρνο περιέχουν ομοιόμορφες λεπτές σχισμές [40].

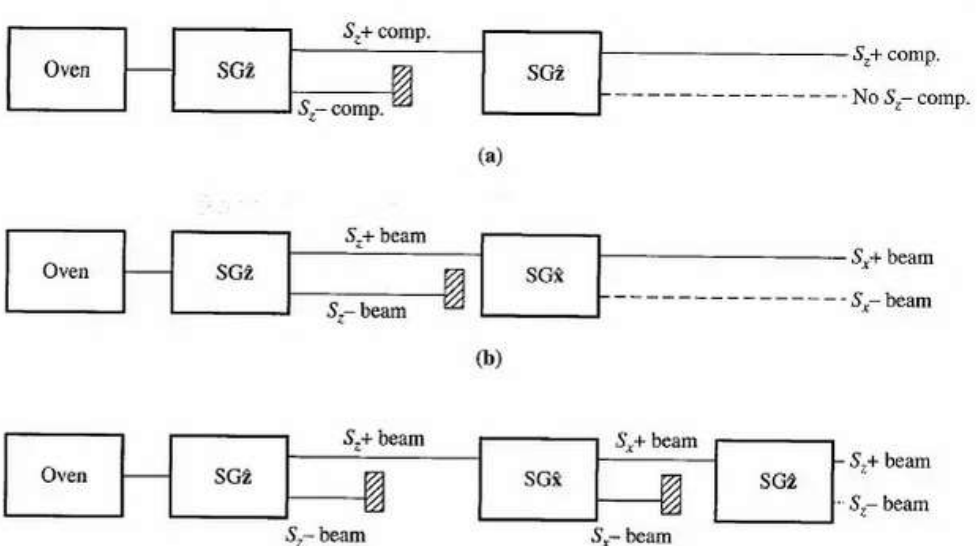
Πώς συμβαίνει αυτό;

Ένα άτομο αργύρου έχει 47 ηλεκτρόνια. 46 βρίσκονται σε ζεύγη όπου του ενός το spin εξουδετερώνει του άλλου. Το τελευταίο ηλεκτρόνιο που περισσεύει μπορεί να βρίσκεται σε οποιαδήποτε κατάσταση (spin up, spin down, superposition spin up & spin down). Όταν το άτομο αργύρου περνάει από το ανομοιογενές μαγνητικό πεδίο, το spin του τελευταίου ηλεκτρονίου αναγκάζεται να πάρει έναν τυχαίο (βασιζόμενο σε πιθανότητες) προσανατολισμό. Είτε στην ίδια κατεύθυνση με το μαγνητικό πεδίο, είτε στην αντίθετη. Έτσι, ανάλογα με την

κατάσταση του τελευταίου ηλεκτρονίου, καθορίζεται η πιθανότητα της μέτρησης του πειράματος να μας δώσει spin up ή spin down [7,38-40].

Όταν διεξήγαγαν το πρώτο πείραμα, οι Stern, Gerlach δεν χρησιμοποίησαν μοναδικά άτομα αργύρου, οπότε δεν μπόρεσαν να επιδείξουν τους πιθανοτικούς κανόνες που διέπουν το πείραμα. Ωστόσο, αποτέλεσαν τη βάση, για να συμβεί αυτό [7,38-40].

Οι συσκευές Stern-Gerlach μπορούν να χρησιμοποιηθούν και για να μετατραπεί η κατάσταση της ακτίνας του ατόμου που περνάει [41].



Εικόνα 6.3: Πώς μια αλληλουχία από SGE μπορεί να τροποποιήσει την κατάσταση μιας ατομικής ακτίνας [41].

6.2 Τα κριτήρια επάρκειας πιθανών τεχνολογιών του DiVincenzo

Σύμφωνα με τα κριτήρια του DiVincenzo, για την κατασκευή ενός πρακτικού κβαντικού υπολογιστή, πρέπει να τηρούνται οι εξής προϋποθέσεις:

Οι πρώτες πέντε, αφορούν τον κβαντικό υπολογισμό:

1. Ένα επεκτάσιμο φυσικό σύστημα με καλώς χαρακτηριζόμενα (well characterized) qubit*
   *Με τον όρο «καλώς χαρακτηριζόμενα» qubits, εννοούμε ότι θα πρέπει να γνωρίζονται όλες οι φυσικές παράμετροί τους.
2. Η δυνατότητα να αρχικοποιείς την κατάσταση των qubit σε μια απλή κατάσταση, η οποία αποτελεί σημείο αναφοράς

3. Μεγάλους, σχετικά, χρόνους κατά τους οποίους η συμπεριφορά ενός συστήματος αλλάζει και πλέον αντί να περιγράφεται από την κβαντομηχανική, περιγράφεται από την κλασσική μηχανική. Σίγουρα μεγαλύτερους από τον χρόνο που παίρνει για να εφαρμοστεί μια κβαντική πύλη (decoherence time).

4. Ένα καθολικό σύνολο (universal set) κβαντικών πυλών*.
   *Επαρκές για να αναπαραστήσει την σειρά από μοναδιαίους μετασχηματισμούς που εφαρμόζονται σε κάποιο αριθμό από qubits, όπως ορίζει ο αντίστοιχος κβαντικός αλγόριθμος.

5. Η δυνατότητα να μπορείς να εκτελέσεις μια μέτρηση σε κάποιο συγκεκριμένο qubit.

Οι υπόλοιπες δύο, αφορούν την κβαντική επικοινωνία (η ανταλλαγή άθικτων qubit από ένα μέρος σε ένα άλλο:

6. Η δυνατότητα να μετατρέπονται το ένα στο άλλο, στατικά (stationary) και ιπτάμενα (flying) qubits*.

7. Η δυνατότητα να μεταδίδονται με εμπιστοσύνη ιπτάμενα qubits μεταξύ συγκεκριμένων τοποθεσιών [42].

*Ιπτάμενα qubits είναι η βέλτιστη υλοποίηση qubits, η οποία θα τους επιτρέπει να χρησιμοποιούνται για την μετάδοση πληροφορίας σε μακρινές αποστάσεις.
Στατικά qubits αποκαλείται η βέλτιστη υλοποίηση qubits για έμπιστους, τοπικούς υπολογισμούς.
Υπάρχει πολύ μεγάλη πιθανότητα, η τεχνολογία υλοποίησης και η επιλογή των σωματιδίων που θα αποτελούν τα ιπτάμενα και στατικά qubits να είναι διαφορετική, καθώς οι απαιτήσεις του κριτηρίου 6 είναι διαφορετικές από αυτές του 7 [42].

6.3 Κβαντικές τεχνολογίες αιχμής για την κατασκευή κβαντικών υπολογιστικών συστημάτων

Καθολικός κβαντικός υπολογιστής ακόμη δεν υπάρχει. Σήμερα γίνονται έρευνες από πολλές ομάδες (Intel, Google, IBM, Microsoft, Rigetti και άλλες) στην προσπάθεια κατασκευής ενός, και

ακολουθούνται πολλές διαφορετικές τεχνολογίες.
Μερικές μόνο από αυτές, είναι οι τεχνολογίες:

- Παγιδευμένων Ιόντων (Trapped Ion Quantum Computer) [43]
- Πυρηνικού Μαγνητικού Συντονισμού (Nuclear Magnetic Resonance Quantum Computing) [44]
- Κβαντικοί Υπολογιστές Σταθερής Κατάστασης Kane (Solid-State NMR Kane) [45]
- Κοιλότητας Κβαντικής Ηλεκτροδυναμικής (Cavity QED) [46]
- Υπεραγώγιμη Κβαντική Υπολογιστικότητα (Superconducting Quantum Computing) [47,48]
- Υπολογιστής Κβαντικής Κουκίδας, βασισμένος σε spin (Quantum Dot Computer) [49,50]
- Οπτικό Πλέγμα (Optical Lattice) [51]
- Κβαντικοί Υπολογιστές Βασισμένοι σε Διαμάντια (Diamond-Based Quantum Computers) [52]
- Μοριακοί Μαγνήτες (Molecular Magnets) [53]
- Γραμμική Οπτική Κβαντική Υπολογιστικότητα (Linear Optical Quantum Computing) [54,55]

Υπάρχει τεράστια ελαστικότητα ακόμη στο ζήτημα της κατασκευής του Κβαντικού Υπολογιστή, ο οποίος βρίσκεται στα νηπιακά του στάδια ακόμη.

Οι κατευθυντήριες οδοί για την δημιουργία ενός κβαντικού υπολογιστή, είναι πάρα πολλές και το ποια θα καταφέρει να νικήσει τα προβλήματα που παρουσιάζει αυτή και να επικρατήσει, άγνωστο.

Δεν θα τις αναλύσουμε καθώς η κάθε μία απαιτεί εξειδικευμένες γνώσης πάνω σε πολλά, περίπλοκα γνωστικά αντικείμενα και ξεφεύγουν από τις δυνατότητές μου.

6.4 Δυναμική διπόλου σε Η/Μ πεδίο

Δίπολο είναι ένα σύστημα που αποτελείται από δύο πράγματα, τα οποία είναι αντίθετα από τη φύση τους και συγκρατούνται μαζί.

Στη φυσική, υπάρχουν δύο ειδών δίπολα (dipole), τα οποία χαρακτηρίζονται από τις στιγμές διπόλου τους (dipole moment):

- Το **ηλεκτρικό δίπολο**, το οποίο είναι ένα ζεύγος ενός θετικού και ενός αρνητικού φορτίου.
  Ροπή ηλεκτρικού διπόλου (Electric Dipole Moment) είναι η μέτρηση της πολικότητας ενός συστήματος (απόσταση μεταξύ του θετικού και του αρνητικού ηλεκτρικού φορτίου του).

- **Μαγνητικό δίπολο** είναι είτε το όριο ενός κλειστού βρόγχου ηλεκτρικού ρεύματος, είτε το όριο ενός ζεύγους μαγνητικών πόλων με αντίθετη πολικότητα. Δεν υπάρχουν στη φύση μαγνητικά μονόπολα.
  Ροπή μαγνητικού διπόλου (Magnetic Dipole Moment) είναι η ροπή που υφίσταται ένα αντικείμενο όταν βρίσκεται σε ένα μαγνητικό πεδίο. Μετράει την τάση ενός αντικειμένου να ευθυγραμμίζεται με ένα μαγνητικό πεδίο. Τέτοια αντικείμενα μπορείνα είναι ένας μόνιμος μαγνήτης, βρόγχοι ηλεκτρικού ρεύματος, κινούμενα στοιχειώδη σωματίδια (π.χ. ηλεκτρόνια).
  Το πιο κλασσικό παράδειγμα που όλοι γνωρίζουμε είναι η πυξίδα, η οποία εισέρχεται στο μαγνητικό πεδίο της γης και δείχνει τον βόρειο και νότιο πόλο του.
  Όταν ένα αντικείμενο τοποθετηθεί μέσα σε ένα μαγνητικό πεδίο και δεν επηρεαστεί, τότε δεν έχει ροπή μαγνητικού διπόλου [56,57].

Μεταβατική ροπή διπόλου (transition dipole moment) d_{nm} μεταξύ μιας κατάστασης m και μιας κατάστασης n είναι η ροπή ηλεκτρικού διπόλου που σχετίζεται με τη μετάβαση μεταξύ των δύο καταστάσεων.
Είναι ένα μιγαδικό διάνυσμα και η κατεύθυνσή της δίνει την πολικότητα της μετάβασης, η οποία καθορίζει πώς το σύστημα θα αλληλεπιδράσει με ένα ηλεκτρομαγνητικό κύμα κάποιας

πολικότητας. Το τετράγωνο του πλάτους της δίνει τη δύναμη της αλληλεπίδρασης λόγω της διανομής του φορτίου μέσα στο σύστημα. Μετριέται σε Cm (Coulomb Meter) ή Debye (D) [56,57].

Spin μαγνητική ροπή (spin magnetic moment) είναι η μαγνητική ροπή διπόλου που προκαλείται από το spin ενός στοιχειώδους σωματιδίου (π.χ. ηλεκτρόνιο – spin 1/2) [56,57].

6.5 Παράδειγμα: Χρήση ατόμων φωσφόρου στη σιλικόνη για δημιουργία εξαρτημάτων ενός κβαντικού υπολογιστή από μια ερευνητική ομάδα

Η ερευνητική ομάδα του Andrea Morello έστρεψε την προσοχή της στην σιλικόνη, η οποία είναι ήδη ευρέως διαδεδομένη για την χρήση της στους κλασσικούς υπολογιστές [58].

Ένα άτομο φωσφόρου ενσωματώνεται σε έναν κρύσταλλο σιλικόνης στο σώμα ενός transistor. Ο πυρήνας αυτού, χρησιμοποιείται ως qubit.

Ας εξετάσουμε πιο απομακρισμένο ηλεκτρόνιο του ατόμου του φωσφόρου. Το ηλεκτρόνιο σε πάρα πάρα πολύ χαμηλές θερμοκρασίες και απομονωμένο περιβάλλον συμπεριφέρεται σαν μια κλασσική πυξίδα, ευθιγραμμίζει το spin του με το μαγνητικό πεδίο στο οποίο βρίσκεται. Με τον ίδιο τρόπο, η πυξίδα ευθιγραμμίζει τους δείκτες της με το μαγνητικό πεδίο της γης. Αυτή είναι η χαμηλότερη ενεργειακή κατάσταση ενός ηλεκτρονίου (spin down).

Για να διαφοροποιήσεις την ενεργειακή κατάσταση του ηλεκτρονίου όταν έχει spin up και spin down πρέπει να εφαρμόσεις ένα ισχυρό μαγνητικό πεδίο. Αυτό μπορείς να το κάνεις με έναν υπεραγωγό μαγνήτη (superconducting magnet). Έτσι, για να μετατρέψεις την κατάσταση με την χαμηλότερη ενέργεια του ηλεκτρονίου, δηλαδή την spin down, στην spin up κατάσταση, απαιτείται κάποια ενέργεια.
Ακριβώς όπως για να αλλάξεις την ευθυγράμμιση των δεικτών της πυξίδας εάν αφαιρέσεις το προστατευτικό γυαλί απαιτείται να χρησιμοποιήσεις κάποια ενέργεια και να την σμπρώξεις με τα χέρια.

Άρα συνοπτικά η διαδικασία έχει ως εξής:
Το ηλεκτρόνιο βρίσκεται σταθερά στην κατάσταση spin down σε ένα περιβάλλον με πάρα πάρα πολύ χαμηλή θερμοκρασία (κοντά στους 0 Kelvin).

Τότε, χτυπώντας το ηλεκτρόνιο με έναν παλμό ενός ηλεκτρομαγνητικού κύμματος με πολύ συγκεκριμένη συχνότητα, η οποία εξαρτάται το ηλεκτρομαγνητικό πεδίο στο οποίο στέκεται το ηλεκτρόνιο (συχνότητα αντίχησης του ηλεκτρονίου (resonance frequency)), μπορείς να το μετατρέψεις στην κατάσταση spin up.
Βέβαια, μπορείς να το μετατρέψεις και σε οποιαδήποτε ενδιάμεση κατάσταση (superposition state), αν σταματήσεις τον παλμό πρόωρα.

Έτσι το ηλεκτρόνιο, από μόνο του, λειτουργεί ως qubit.

Πώς μπορούμε να μετρήσουμε, ωστόσο, την κατάσταση του ηλεκτρονίου, με αυτήν την τεχνική, στην συνέχεια;

Όταν το ηλεκτρόνιο βρίσκεται στην spin up κατάσταση, αποδεσμεύεται από το άτομο φωσφόρου και μεταφέρεται στο transistor. Τώρα το άτομο φωσφόρου έχει θετικό φορτίο. Έτσι, και η πύλη του transistor πλέον έχει αυξημένα θετική τάση, λόγω αυτού του ατόμου. Έτσι, στη φάση μέτρησης στο παλμοσκόπιο, μία αιχμή ρεύματος υποδηλώνει ότι το ηλεκτρόνιο βρισκόταν στην κατάσταση spin up, ενώ η απώλεια αυτής σημαίνει spin down.

Ωστόσο αυτή η ομάδα χρησιμοποίησε και τον ίδιο τον πυρήνα του ατόμου φωσφόρου ως qubit, καθώς επειδή έχει πολύ πιο ασθενές spin, έχει πολύ μεγαλύτερη διάρκεια ζωής.

Ο πυρήνας χρειάζεται διαφορετική ηλεκτρομαγνητική ακτινοβολία για να μετατραπεί στην κατάσταση spin up. Επιπλέον, ο ίδιος προκαλεί ένα εσωτερικό μαγνητικό πεδίο, το οποίο μπορεί να δείχνει πάνω ή κάτω και στην ουσία επιδεικνύει στο πιο απομακρυσμένο ηλεκτρόνιο σε ποια ηλεκτρομαγνητική ακτινοβολία να αντιδράσει. Έτσι, μπορούμε να διαβάσουμε την κατάσταση του πυρήνα στο παλμοσκόπιο, μέσω των αιχμών του ηλεκτρονίου. Ύπαρξη αιχμών σημαίνει spin up, ενώ απώλεια σημαίνει spin down [58].

ΚΕΦΑΛΑΙΟ 7

Προβληματισμοί

Υπολογίζεται ότι ο αριθμός qubit τα οποία θα έπρεπε να χειρίζεται ένας κβαντικός υπολογιστής για να είναι χρήσιμος και ανταγωνιστικός με τους κλασσικούς, τους οποίους λειτουργούμε είναι ανάμεσα στα 1,000 και 100,000. Τότε, η κατάσταση που θα περιέγραφε το σύστημά μας ανά πάσα στιγμή θα περιείχε τουλάχιστον 2^{1000} παραμέτρους (πλάτη πιθανότητας). Ο αριθμός αυτός είναι αφάνταστα μεγάλος. Για την ακρίβεια, είναι πολύ μεγαλύτερος από τον αριθμό των υποατομικών σωματιδίων στο παρατηρήσιμο σύμπαν. Αυτά όλα, χωρίς να λάβουμε υπόψιν τα qubits που απαιτούνται για διόρθωση σφαλμάτων στον οποιοδήποτε αλγόριθμο. Αυτά μπορεί να είναι από 1,000 έως 100,000 για κάθε qubit.

Σε τι αριθμό qubits βρισκόμαστε αυτήν την στιγμή;
Οι τρεις μεγαλύτερες εταιρίες στον τομέα, Intel, IBM, Google πειραματίζονται με κβαντικούς υπολογιστές ισχύος 49-qubit, 53-qubit και 72-qubit αντίστοιχα.

Υπάρχει ένα τεράστιο κενό ανάμεσα στο τι καθίσταται εφικτό από τους κανόνες της κβαντομηχανικής και της κβαντικής-υπολογιστικής θεωρίας, η οποία επιτρέπει θεωρητικά τον χειρισμό εξαιρετικά πολύπλοκων κβαντικών συστημάτων και το τι μπορούμε να κατασκευάσουμε χρησιμοποιώντας υλικά στον πραγματικό, φυσικό κόσμο [59].

ΚΕΦΑΛΑΙΟ 8

Κβαντική Υπεροχή (Quantum Supremacy)

Κβαντική υπεροχή είναι η πρακτική επίδειξη μιας προγραμματισμένης κβαντικής συσκευής, η οποία να λύνει ένα πρόβλημα, το οποίο ένας κλασσικός υπολογιστής δεν θα μπορούσε (εντός ενός λογικού χρόνου), ανεξαρτήτως της χρησιμότητας του προβλήματος [60].

Στις 23 Οκτωβρίου 2019, η Google ανακοίνωσε πως πέτυχε αυτόν το στόχο, εκτελώντας σε έναν κβαντικό υπολογιστή 53 qubit μια σειρά από πράξεις σε 200 δευτερόλεπτα, οι οποίες σε έναν κλασσικό υπολογιστή θα έπαιρναν 10,000 χρόνια. Ωστόσο, το πρόβλημα το οποίο επίλυσε, δεν έχει κάποια ιδιαίτερη σημαντικότητα ή πρακτική εφαρμογή [61].

Το είδος qubits που χρησιμοποίησε αποκαλούνται υπεραγώγιμα “transmon” qubits [62].

Η IBM αντέδρασε με σκεπτικισμό, χαρακτηρίζοντας τους ισχυρισμούς της Google υπερβολικούς, καθώς το πρόβλημα μπορεί να προσομοιωθεί ιδανικά σε έναν κλασσικό υπολογιστή, με μεγαλύτερη πιστότητα, σε 2.5 ημέρες. Σύμφωνα με την IBM, για αυτόν τον λόγο, η κβαντική υπεροχή δεν έχει ακόμη επιδειχθεί [63].

ΚΕΦΑΛΑΙΟ 9

Συμπεράσματα

Θα καταφέρει η ανθρωπότητα να κατασκευάσει έναν καθολικό κβαντικό υπολογιστή ή θα εγκαταλείψει αυτήν της την προσπάθεια; Οι αμφισβητίες αυτής της προσπάθειας είναι δικαίως πολλοί. Οι απαιτήσεις σε αριθμό qubit φαίνονται να είναι τεράστιες, η έρευνα πολυετής και αφηρημένες έννοιες όπως ο «προφήτης» που φαίνεται να έχουν μαγικές ιδιότητες δεν βοηθάνε. Επιπλέον, οι δυνατότητες να ασχοληθεί κανείς με αυτόν τον τομέα είναι λίγες, καθώς δεν υπάρχουν πολλοί προσβάσιμοι κβαντικοί υπολογιστές. Αν προσθέσεις σε αυτά και το γεγονός ότι είναι ένα εξαιρετικά περίπλοκο αντικείμενο, και για να ασχοληθείς με αυτό πρέπει να έχεις πολυεπίπεδες γνώσεις διαφορετικών γνωστικών αντικειμένων, τα εμπόδια φαντάζουν πολλά.

Ωστόσο, εγώ προσωπικά, δεν θα στοιχημάτιζα εναντίον μας. Η υπολογιστική ισχύς που υπόσχεται ένας κβαντικός υπολογιστής είναι τεράστια και τα οικονομικά κίνητρα των εταιριών που ασχολούνται με αυτό, κυρίως λόγω της υπόσχεσης στον τομέα της κβαντικής κρυπτογραφίας, είναι τεράστια. Επιπλέον, πριν 50 χρόνια ποιος θα φανταζόταν τα ακραία τεχνολογικά επιτεύγματα του σήμερα και πριν 100 χρόνια ποιος θα φανταζόταν αυτά που υπήρχαν πριν 50. Έχει ήδη αποδειχθεί επανειλημμένα ότι εάν η ανθρωπότητα βάλει στο μυαλό της κάτι και επενδύσει σε αυτό, κανένα εμπόδιο δεν είναι υπερβολικά μεγάλο.

ΒΙΒΛΙΟΓΡΑΦΙΚΕΣ ΑΝΑΦΟΡΕΣ

1. Nottale L, Célérier M. Derivation of the postulates of quantum mechanics from the first principles of scale relativity. Journal of Physics A: Mathematical and Theoretical. 2007;40(48):14471-14498.
2. Lvovsky A. The quantum postulates. Quantum Physics. 2018;:1-39.
3. Γούσια Π. ΚΒΑΝΤΙΚΟΙ ΥΠΟΛΟΓΙΣΤΕΣ: Μέθοδοι υλοποίησης κβαντικών πυλών. Διπλωματική εργασία, Αριστοτέλειο Πανεπιστήμιο Θεσσαλονίκης, Τμήμα Πληροφορικής; 2015.
4. Ταμβάκης Κ. Εισαγωγή στην Κβαντομηχανική. Β' έκδοση. Εκδόσεις Leader Books; 2003.
5. Loceff M. A Course in Quantum Computing. Foothill College; 2015.
6. Dirac P. THE PRINCIPLES OF QUANTUM MECHANICS. 3rd ed: Oxford University Press; 1947
7. Τραχανάς Σ. Κβαντομηχανική ΙΙ. Πανεπιστημιακές Εκδόσεις Κρήτης; 2016.
8. Nielsen M, Isaac L Chuang. Quantum Computation and Quantum Information. 10th ed: Cambridge University Press; 2010.
9. Καραφυλλίδης Ι. Κβαντική Υπολογιστική. Ελληνικά Ακαδημαϊκά Ηλεκτρονικά Συγγράματα και Βοηθήματα; 2015.
10. Einstein A, Podolsky B, Rosen N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?. Physical Review. 1935;47(10):777-780.
11. Bohr N. Can Quantum-Mechanical Description of Physical Reality be Considered Complete?. Physical Review. 1935;48(8):696-702.
12. Ambainis A. Quantum search algorithms. ACM SIGACT News. 2004;35(2):22.
13. Shor P. Algorithms for quantum computation: discrete logarithms and factoring. Proceedings 35th Annual Symposium on Foundations of Computer Science. 1994.
14. Hayward M. Quantum Computing and Shor's Algorithm. 2015.
15. Wiesner S. Conjugate coding. ACM SIGACT News. 1983;15(1):78-88.

16. Ekert A. Quantum cryptography based on Bell's theorem. Physical Review Letters. 1991;67(6):661-663.

17. Viola L, Knill E, Laflamme R. Constructing qubits in physical systems. Journal of Physics A: Mathematical and General. 2001;34(35):7067-7079.

18. Shaw B, Wilde M, Oreshkov O, Kremsky I, Lidar D. Encoding one logical qubit into six physical qubits. Physical Review A. 2008;78(1).

19. Bisht P, Some S. Quantum Error Correction. 2017.

20. Devitt S, Munro W, Nemoto K. Quantum error correction for beginners. Reports on Progress in Physics. 2013;76(7):076001.

21. Roffe J. Quantum error correction: an introductory guide. Contemporary Physics. 2019;60(3):226-245.

22. Babar Z, Chandra D, Nguyen H, Botsinis P, Alanis D, Ng S et al. Duality of Quantum and Classical Error Correction Codes: Design Principles and Examples. IEEE Communications Surveys & Tutorials. 2019;21(1):970-1010.

23. Shor P. Scheme for reducing decoherence in quantum computer memory. Physical Review A. 1995;52(4):R2493-R2496.

24. Eastin B, Flammia S T. Q-circuit Tutorial. Department of Physics and Astronomy, University of New Mexico. 2004.

25. Preskill J. FAULT-TOLERANT QUANTUM COMPUTATION. California Institute of Technology. 1997.

26. Gottesman D, Preskill J. Stabilizer codes and quantum error correction. Pasadena, Calif.: California Institute of Technology; 1997.

27. Ziemer R, Tranter W. Principles of communications. 7th ed. Wiley; 2014.

28. Touchette D, Ali H, Hilke M. 5-qubit Quantum error correction in a charge qubit quantum computer. 2010.

29. Niwa j, Matsumoto K, Imai H. Simulating the Effects of Quantum Error-correction Schemes. 2018.

30. Laflamme R, Miquel C, Paz J, Zurek W. Perfect Quantum Error Correcting Code. Physical Review Letters. 1996;77(1):198-201.

31. Gottesman D. Quantum Error Correction and Fault Tolerance. Encyclopedia of Mathematical Physics. 2006;:196-201.

32. Katabarwa A, Geller M. Logical error rate in the Pauli twirling approximation. Scientific Reports. 2015;5(1).

33. Steane A. Multiple-particle interference and quantum error correction. Proceedings of the Royal Society of London Series A: Mathematical, Physical and Engineering Sciences. 1996;452(1954):2551-2577.

34. Dong P, Liu J, Cao Z. Efficient Quantum Circuit for Encoding and Decoding of the [[8,3,5]] Stabilizer Code. International Journal of Theoretical Physics. 2012;52(4):1274-1281.

35. Fowler A, Stephens A, Groszkowski P. High-threshold universal quantum computation on the surface code. Physical Review A. 2012;80(5).

36. Bravyi S B, K A U. Quantum codes on a lattice with boundary. 1998;2.

37. Steane A. A Tutorial on Quantum Error Correction. 2006;162.

38. Gerlach W, Stern O. Der experimentelle Nachweis der Richtungsquantelung im Magnetfeld. Zeitschrift fur Physik. 1922;9(1).

39. Schmidt-Böcking H, Schmidt L, Lüdde H, Trageser W, Templeton A, Sauer T. The Stern-Gerlach experiment revisited. The European Physical Journal H. 2016;41(4-5):327-364.

40. Wennerström H, Westlund P. The Stern–Gerlach experiment and the effects of spin relaxation. Phys Chem Chem Phys. 2012;14(5):1677-1684.

41. Sakurai J, Napolitano J. Modern quantum mechanics. Reading, Mass.: Addison-Wesley; 2011.

42. DiVincenzo D. The Physical Implementation of Quantum Computation. Fortschritte der Physik. 2000;48(9-11):771-783.

43. Blinov B, Leibfried D, Monroe C, Wineland D. Quantum Computing with Trapped Ion Hyperfine Qubits. Quantum Information Processing. 2004;3(1-5):45-59.

44. Gershenfeld N, Chuang I. Quantum Computing with Molecules. Scientific American. 1998;278(6):66-71.

45. Kane B. A silicon-based nuclear spin quantum computer. Nature. 1998;393(6681):133-137.

46. Walther H, Varcoe B, Englert B, Becker T. Cavity quantum electrodynamics. Reports on Progress in Physics. 2006;69(5):1325-1382.

47. Kaminsky W, Lloyd S, Orlando T. Scalable Superconducting Architecture for Adiabatic Quantum Computation. 2004.

48. Clarke J, Wilhelm F. Superconducting quantum bits. Nature. 2008;453(7198):1031-1042.

49. Imamog¯lu A, Awschalom D, Burkard G, DiVincenzo D, Loss D, Sherwin M et al. Quantum Information Processing Using Quantum Dot Spins and Cavity QED. Physical Review Letters. 1999;83(20):4204-4207.

50. Loss D, DiVincenzo D. Quantum computation with quantum dots. Physical Review A. 1998;57(1):120-126.

51. Brennen G, Caves C, Jessen P, Deutsch I. Quantum Logic Gates in Optical Lattices. Physical Review Letters. 1999;82(5):1060-1063.

52. Nizovtsev A et al. A Quantum Computer Based on NV Centers in Diamond: Optically Detected Nutations of Single Electron and Nuclear Spins. Optics and Spectroscopy. 2005;99(2):233.

53. Leuenberger M, Loss D. Quantum computing in molecular magnets. Nature. 2001;410(6830):789-793.

54. Knill E, Laflamme R, Milburn G. A scheme for efficient quantum computation with linear optics. Nature. 2001;409(6816):46-52.

55. Adami C, Cerf N. Quantum Computation with Linear Optics. Quantum Computing and Quantum Communications. 1999;:391-401.

56. Serway R, Jewett J. Physics for scientists and engineers. 6th ed. Pacific Grove, Calif.: Thomson-Brooks/Cole; 2004.

57. Cullity B, Graham C. Introduction to Magnetic Materials. 2nd ed. Hoboken: Wiley; 2009.

58. Pla J, Tan K, Dehollain J, Lim W, Morton J, Zwanenburg F et al. High-fidelity readout and control of a nuclear spin qubit in silicon. Nature. 2013;496(7445):334-338.

59. 4. Dyakonov M. The Case Against Quantum Computing [Internet]. IEEE Spectrum: Technology, Engineering, and Science News. 2018 [cited 11 February 2020]. Available from: https://spectrum.ieee.org/computing/hardware/the-case-against-quantum-computing

60. Preskill J. Quantum computing and the entanglement frontier. Rapporteur talk at the 25th Solvay Conference on Physics. 2012.

61. Arute F, Arya K, Babbush R, Bacon D, Bardin J, Barends R et al. Quantum supremacy using a programmable superconducting processor. Nature. 2019;574(7779):505-510.

62. Koch J, Yu T, Gambetta J, Houck A, Schuster D, Majer J et al. Charge-insensitive qubit design derived from the Cooper pair box. Physical Review A. 2007;76(4).

63. Pednault E, Gunnels J, Maslov D, Gambetta J. On “Quantum Supremacy” [Internet]. IBM Research Blog. 2019 [cited 11 February 2020]. Available from: https://www.ibm.com/blogs/research/2019/10/on-quantum-supremacy/

Ορολογία - Γλωσσάρι

Μεταφράσεις σημαντικών όρων

Αναμενόμενη Τιμή : Expectation Value

Κυματοσυνάρτηση : Wave function

Παρατηρήσιμο : Observable

Προφήτης : Oracle

Τελεστής : Operator

Ιδιοστροφορμή : Spin

Ερμιτιανός : Hermitian

Ιδιοτιμή : Eigenvalue

Ιδιοδιάνυσμα : Eigenvector

Ιδιοκατάσταση : Eigenstate

Μεταθέτης & Αντιμεταθέτης : Commutator & anti-Commutator

Πλάτος : Amplitude

Συζυγής : Conjugate

Φασματική Ανάλυση: Spectral Decomposition

Υπέρθεση : Superposition

Συχνοί συμβολισμοί

Αν A είναι ένας πίνακας:

- A^* *: Συζυγής πίνακας του A*
- A^T *: Ανάστροφος πίνακας του A (ομοίως για διανύσματα)*
- A^H ή A^t *: Ερμιτιανός ανάστροφος πίνακας του A (ομοίως για διανύσματα)*

$\bar{x}$: Μέση τιμή του x